حروب الفضاء الالكتروني وعلاقتها بحروب الجيل الخامس

الأستاذ الدكتور / محمود محمد علي

أستاذ الفلسفة/ جامعة أسيوط



المقدمة

ذكرنا في كتاباتنا عن حروب الجيل الخامس،أنها تستخدم العنف المسلح عبر مجموعات عقائدية مسلحة، وعصابات التهريب المنظم والتنظيمات الصغيرة المدربة صاحبة الأدوار المنهجة؛ حيث يستخدم فيها من تم تجنيدهم بالتكنولوجيا المتقدمة، والسبل الحديثة لحشد الدعم المعنوي والشعبي. والاختلاف بينها وبين الجيل الرابع هو أن الجيل الرابع كان يعتمد على تقنيات حرب اللاعنف، لكن الجيل الخامس يستخدم العنف بشكل رئيسي معتمداً على التقنيات الحديثة. ويُقصد بالتكنولوجيا المتقدمة الأسلحة المتطورة، والتي استخدمت ضمن تكتيكات وأساليب "الحرب الهجينة" التي تتداخل فيها وتتمازج أصناف وطرق وأنماط متعددة من الحروب. فمن وسائل الحرب التقليدية المعروفة (دبابات وصواريخ ومدافع وطائرات) إلى وسائل وطرق

وقتال العصابات وأعمال حرب الإرهاب ونشر الرعب بأبشع صوره.

كما أبرزنا أيضاً في في كتاباتنا أن الحرب الهجينة، هي استراتيجية فاعلة للحروب، دخلت ضمن المصطلحات العسكرية الحديثة للحروب، تتجه لتكون أسلوباً ثورياً في المفاهيم المعتادة للحرب، مع أنها عملياً تعتبر قديمة متجددة، فهي تعتبر نوعاً متميزاً من القتال الذي يعجز فيه الجيش النظامي عن الإطاحة بعدو يعتقد أنه غير محترف، ويخوض حرباً غير نظامية، بأفكار مبتكرة هي خليط من مفهوم الحرب الشعبية أو الحرب الثورية وأسلوب حرب العصابات، وتعد وسائل هذه الحرب حديثة تتمتع بتكنولوجيا فائقة لا تخضع لشكل معين أو قواعد ثابتة بداية من القيادة وانتهاء بالعمليات الجارية خلالها الآن، وهدف هذه الحرب الهجينة هو تحطيم قوة العدو وشل قدراته، وإنزال أكبر الخسائر في قواته، وهي بذلك تخالف تماماً القواعد والأسس المتعارف عليها

في الحروب سابقاً، لأنها لا تسير وفق نهج ومبادئ القتال الرئيسية التقليدية التي تشكل الأساس الفكري لأغلب جيوش العالم، بل تعدت ذلك لتصبح شكلاً ونمطاً مغايراً للصراع الذي لم يعد فيه القتال حكراً على الجيوش النظامية وعلى مهارات العسكريين المحترفين لتكون هذه الحرب الهجينة خليطا من وحشية النزاع النظامي الذي تخوضه الدول مع أصولية الحرب غير النظامية ونفَسها الطويل التي تعتمدها القوات غير النظامية.

كما ناقشنا أيضاً في كتاباتنا كيف أن هذه الحروب «الهجينة» هي «حروب بديلة» ومركبة"، تخوضها قوى كبرى بواسطة لاعبين أصغر، بعد استغلال التناقضات وتأجيجها وتخصيب الاختلافات الفكرية والدينية والمذهبية والإثنية داخل المكونات المتعددة في مجتمع ما أو دولة ما، للوصول إلى أهداف استراتيجية وتحقيق مصالح وغايات الدول الكبرى وتجار الحروب.

وقد بينا في كتاباتنا كيف تطول هذه الحروب وتستمر حتى تدمير جيوش بعض الدول وتقسيم مجتمعاتها وتغيير أنظمتها السياسية أو خرائطها الجغرافية أو حتى التوصل إلى تسويات واتفاقات جيوستراتيجية على مستوى الإقليم والعالم. لذلك، يمكن القول أنّ الحرب الهجينة، هي بالنسبة الى بعض الدول الكبرى، بديل عن الحروب التقليدية التي تُخاض بالوسائل العسكرية الذاتية، لأنّ أكلافها ونتائجها ستكون كارثية عليها وعلى مصالحها في حال خاضتها بصورة علنية ومباشرة.

من ناحية أخري أبرزنا في في كتاباتنا أنه في الحرب الهجينة تواجه خصماً عنيداً في تشكيلات عسكرية أو شبه عسكرية غير نظامية تتنادى لتطور المواجهة لمقاومة غزو أجنبي دون تدريب رسمي، حيث تبرز في هذه المواجهة قوة المشاركة المباشرة للسكان في حالة القتال دفاعاً عن النفس والأرض، أو قد تنزلق نحو حرب أهلية

يخوض فيها المقاتلين قتالاً شرساً تحكمهم توجهاتهم الفكرية والجهوية، وفي هذا الصدد يكون الدخول في حرب غير تقليدية من أجل تقويض سلطة للعدو وإضعاف إرادته هو السبيل للمقاومة، وهنا تفشل كل خطط الحرب التقليدية لتدخل حسابات جديدة في المعادلة؛ حيث يختلف الأسلوب القتالي في إدارة الحرب عن قبل، وبذلك تتغير النتائج وتظهر مع الوقت صعوبة المواجهة مع خصم يظهر ويختفي، ويضرب متى شاء، وكيفما شاء بكل اقتدار ونجاح.

كما تعتمد أساليب القوات غير النظامية، غالباً على حرب العصابات، وعمليات حرب المدن، وإعداد الكمائن، واستهداف مواقع استراتيجية مؤثرة، وهذا يستدعي تجنب التورط بالدخول في معارك، ومجابهات على نطاق واسع، والتركيز على الاشتباكات الصغيرة، وعمليات التمويه والكر والفر، واستخدام وسائل، قد تكون بدائية مع وسائل أكثر تطوراً، حسب الحاجة مع

تطور طبيعة الصراع، لتأخذ أشكالاً أكثر تعقيداً، تلبية للتطور الحاصل في الوسائل التكنولوجية والمعلوماتية، التي أوجدت مجالات جديدة للمواجهة لتحقيق أهدافها.

يندمج في الحرب الهجينة أنماط القتال المعروفة المختلفة، بما في ذلك القدرات التقليدية، وأساليب القتال المستحدثة، والتكتيكات، والأعمال الفدائية، للاستفادة من كل أشكال القتال المشروعة، لاستنزاف وإرهاق الخصم، لإرغامه علي الانسحاب من أراض محتلة، أو التخلي عن سياسة خارجية معينة.

وانهينا حديثا في في كتاباتنا ، بأن أخطر أشكال الحروب التي تواجهها المجتمعات والدول النامية، والتي بدأت في الظهور خلال العقد الأول من القرن الحادي والعشرين، هي ما يطلق عليها الحروب «الهجينة». وهي الحروب القائمة على المساحة، التي تلتقي فيها حروب

الفضاء الكوني مع حروب الفضاء الرقمي، وتكون نتيجتها خسائر مضاعفة بمئات المرات، مقارنة بالحروب التي تقتصر على إحدى الساحتين بشكلٍ منفصل. والسبب الرئيس وراء ذلك، هو اعتماد الحروب "الهجينة" على أسلحة ووسائل وأدوات تقليدية وغير تقليدية، منتظمة وغير منتظمة، علنية وخفية، ويتم فيها استغلال كل الأبعاد الجديدة في هذه الحروب، للتغلب على التفوق الذي تمتلكه الدول في الحروب التقليدية، وأهمها على الإطلاق البعد الذي أضافه الفضاء الرقمي إلى المنظومة البشرية التقليدية.

وفي هذا الكتاب نحاول أن نكمل المسيرة، فنتحدث عن دور الفضاء الإلكتروني في تأجيج صراعات حروب الجيل الخامس، حيث يذكر بعض الباحثين أنه عادة ما تتشكل الجيوش الحربية الحديثة من ثلاثة أذرع، وهي القوة الجوية والقوة البرية، والقوة البحرية تستخدمها للهجوم علي أعدائها والدفاع عن أرضها. ولكن في عصر

الانترنت والاتصالات، بدأنا نسمع عن معارك يدور رحاها في الفضاء الالكتروني، وبين خصوم معظمهم مجهول الهوية، يهاجمون البنية التحتية الرقمية، للدول التي يصفونها في خانة العدو؛ حيث "تهدف الهجمات الرقمية إلي الحصول علي معلومات مخابراتية حساسة، أو تدمير بنية الاقتصاد الذي بدأ يعتمد علي المعلومات بشكل كبير، أو لمجرد إشعار أنهم موجودون علي الجبهة الرقمية، وبإمكانهم إزعاجه" (١).

لقد أصبح عصرنا الحالي يتصف بعصر الثورة الرقمية والإلكترونية، وأداة هذا العصر هي وسائل الاتصال الإلكترونية. دخلت هذه الوسائل جميع مجالات الحياة الإنسانية بشكلٍ قوي، وأصبحت أداةً للتغيير تستخدمها كافة شُعوب العالم في شتى المجالات، كما أضحت وسيلةً قويةً تستخدمها شُعوب الأرض دون أن تحرك جيوشها، أو تُهدر أموالها، الأمر الذي جعل منها سلاحاً للتهديد والردع والرد. فعبر شاشة الحاسوب، "تستطيع

الدول أن تُدمر البنية التحتية لأي عدوٍ يواجهها، مستخدمةً لذلك حرباً إلكترونية، ومنظومةً معلوماتيةً وتّقنية، وهجماتٍ حاسوبيةً باتت تؤرق الكثير من دول العالم" (٢).

إن الحروب الإلكترونية باتت مجالاً جديداً للحرب والقتال، حيث أضحت الدول المتطورة تزيد من نشاطاتها وأبحاثها في الفضاء الالكتروني، "والذي أصبح يشكل بالنسبة لها مصدر قوة، لكنه في الوقت نفسه يكشف عن خاصرتها الضعيفة، لأن البنية التحتية التي تقوم عليها الدول الحديثة، كالاتصالات والنظم الدفاعية، والأمنية، والمالية، والاقتصادية، والتنموية، تعتمد في عملها وبشكلٍ كبير على الفضاء الالكتروني المحوسب" (٣).

وأصبح الفضاء الإلكتروني ساحة جديدة للصراع بشكله التقليدي، ولكنه "ذو طابع إلكتروني يعكس

النزاعات التي تخوضها الدول أو الفاعلين من غير الدول على خلفيات دينية، أو عرقية، أو إيديولوجية، أو اقتصادية، أو سياسية. ويتمدد الصراع الإلكتروني بداخل شبكات الاتصال والمعلومات، متجاوزا الحدود التقليدية، وسيادة الدول، ويؤثر ذلك في امتداد مجاله، وتداعياته، أو آثاره، وأضافت عملية تعدد الاستخدام والفاعلين والمصالح لتنوع أشكال الصراع وأهدافه" (٤).

ولأن الصراعات "الفعلية" تستعمل شتى أنواع أسلحة التدمير الاقتصادية، والإلكترونية، والسياسية، والإعلامية، فإنها "لم تتوان عن استخدام الفضاء الالكتروني، بما له من تأثير نفسي، ومعنوي، وإعلامي، ثم أصبح له تأثير أمني، وعسكري، لتزحف جبهات القتال التقليدية، بشكل مواز لها إلى ساحة الفضاء الإلكتروني"(٥).

وكشف استخدام الفضاء الإلكتروني عن حالة التعارض الحقيقي، أو المتخيل، للاحتياجات، والقيم، والمصالح بين العديد من الفرقاء، سواء أكانوا دولاً، أو أفراداً، أو جماعات، أو شركات، "وبما ساعد على بلورة أساليب للصراع الدولي ذات الطابع التقني، والتجاري، والاقتصادي، والعسكري، إلى جانب ظهور طرق بديلة عن الحرب المباشرة بين الدول، أو بين الخصوم عبر شبكات الاتصال والمعلومات"(٦).

وكان لتلك التغييرات دور في إعادة التفكير في حركية وديناميكية الصراع والأمن، على نحو يعكس التطور الذي فرضه الفضاء الإلكتروني على المجتمع الدولي، وخاصة في ظل تزايد حالة الاعتماد المتبادل، وهو ما ساعد في ظهور ما يعرف" بـ "عصر القوة النسبية" الذي يعني بعجز" القوة العسكرية" عن تأمين الأهداف السياسية المترتبة عليها، مما يخلف آثاراً استراتيجية هائلة على مستوى تركيبة وتوازنات النظام الدولي" (٧).

وذلك بعد أن تغير "براديم" الحرب جذرياً بانتقاله من نسق "الحروب الصناعية بين الدول" إلى نسق "الحرب في وسط الشعوب". ففي الحروب القديمة كان الغرض هو تدمير الخصم، إما باحتلال أرضه، أو الاستيلاء على موارده، بينما أصبح في الحرب الجديدة، هو التحكم في إرادته وخياراته، ومن ثم كان الدور المحوري للشعوب في هذا الصنف الجديد من الحروب، سواء تعلق الأمر بالسكان المستهدفين في أرضية المواجهة، أو بالرأي العام في الدولة التي تشن الحرب، أو بالرأي العام الإقليمي والدولي. وأصبحت أهداف الحرب أقل مادية، يؤدي فيها العامل النفسي والدعائي دوراً محورياً، وسببه تنامي التغطية الإخبارية السمعية البصرية المباشرة، للأحداث لحظة وقوعها عبر مواقع الإنترنت والفضائيات، إلى جانب ضعف سيطرة أنظمة الحكم على توجهات مواطنيها.

وعلى الرغم من سعى الجيوش النظامية لاستغلال تفوقها التقني العسكري - الإعلامي الكاسح، لحسم حرب نظيفة سريعة تجنب السكان فظائع وآلام المواجهة، فإن استراتيجية الشبكات الإلكترونية المسلحة المقاومة لها هي "الاستخدام المعاكس لهذه الميزات التقنية، إلى جانب اتباع استراتيجية مواجهة متدرجة تؤدي إلى إنهاك الخصم للتغلب عليه بالتسلل إلى وسط السكان والاحتماء بهم، وزعزعه ثقتهم في مؤسسات الدولة، وبالتالي تحويلهم إلى أرضية مواجهة بديلة عن المواجهة المباشرة بين دول، ويتم في ذلك توجيه سلاح الصورة إلى مآسي الحرب وجرائمها الإنسانية، بما يعمل على شحن الرأي العام، وهو ما برز بظهور فكرة "إسقاط النظام من الداخل" بدلاً من استخدام القوة العسكرية الخارجية كحالة العراق "(٨).

وفي هذا المشهد تتمحي الفروق التقليدية بين الحرب والسلم، ففي الوقت الذي يغدو فيه الصدام السمة الغالبة

على الوضع الاستراتيجي الدولي فإنه أفرز تعاوناً متبادلاً ، وإن كان نادراً ما يتطور إلى "حالة مواجهة مسلحة للوعي المتزايد بعدم قدرة الحسم العسكري في إطفاء بؤر التوتر القائمة. وتم توظيف التطرف ذي الخلفيات الدينية أو القومية لتحويل استخدام التكنولوجيا من أداة مدنية إلى أداة عسكرية وذات أبعاد تخريبية" (٩).

ومن أهم أشكال الصراع في عصر المعلومات هما" حرب الشبكات وحرب الفضاء الإلكتروني Cyber war & Net war وعلى الرغم من زيادة معدلات استخدام تلك الأشكال، إلا أن ذلك لا يعني بالضرورة اعتمادها فقط وسائل تكنولوجيا الاتصال والمعلومات، بل تأتي مواكبة أو معبرة عن استخدام الآليات التقليدية للصراع، ولكن بوجه تكنولوجي يتواكب مع عصر المعلومات" (١٠).

ويتميز الصراع الإلكتروني Cyber Conflict بأن به تدمير لا تصاحبه دماء وأشلاء بالضرورة، يتضمن التجسس والتسلل، ثم النسف، لكن لا دخان، ولا أنقاض، ولا غبار، ويتميز "أطرافه بعدم الوضوح، وتكون تداعياته خطيرة، سواء عن طريق تدمير المواقع على الإنترنت ونسفها وقصفها بوابل من الفيروسات، أو العمل على استخدام أسلحة الفضاء الإلكتروني المتعددة، للنيل من سلامة تلك المواقع، وهي أسلحة يسهل الحصول عليها من خلال مواقع الإنترنت أيضاً وتعلم كيفية استخدامها كما إن انتشار الفضاء الإلكتروني وسهولة الدخول إليه، يمكن أن يوسع دائرة استهداف المواقع، بالإضافة إلى زيادة عدد المهاجمين، ولتدور تلك الهجمات المتبادلة على نحو من الكر والفر ليعبر عن حالة صراع ممتد يرتبط بطبيعة الفضاء الإلكتروني المختلفة" (١١).

وهناك صراع إلكتروني تحركه دوافع سياسية ويأخذ شكلاً عسكرياً، ويتم فيه استخدام قدرات هجومية، ودفاعية عبر الفضاء الإلكتروني، وذلك بهدف إفساد النظم المعلوماتية، والشبكات، والبنية التحتية، وبما يتضمن استخدام أسلحة، وأدوات إلكترونية، من قبل فاعلين داخل المجتمع المعلوماتي، أو من خلال التعاون، ما بين قوى أخرى، لتحقيق أهداف سياسية. كما أن هناك صراع إلكتروني "ذو طبيعة ناعمة عن طريق الصراع حول الحصول على المعلومات، والتأثير في المشاعر، والأفكار وشن حرب نفسية واعلامية، ويتم أيضاً من خلال تسريب المعلومات، واستخدامها عبر منصات إعلامية، بما يؤثر على طبيعة العلاقات الدولية، كالدور الذي لعبه موقع ويكيليكس في الدبلوماسية الدولية" (١٢).

ويأخذ الصراع الإلكتروني طابعا تنافسيا حول الاستحواذ على سباق التقدم التكنولوجي، وسرقة

الأسرار الاقتصادية والعلمية، إلى أن يمتد ذلك الصراع إلى محاولة السيطرة على الإنترنت من خلال السعي للسيطرة على أسماء النطاقات وعناوين المواقع، والتحكم بالمعلومات،" والعمل على اختراق الأمن القومي للدول بدون استخدام طائرات، أو متفجرات، أو حتى انتهاك للحدود السيادية، كهجمات قراصنة الكمبيوتر، وتدمير المواقع والتجسس، بما يكون له من تأثير على تدمير الاقتصاد والبنية التحتية بنفس القوة التي قد يسببها تفجير تقليدي مدمر" (١٣) ؛ وخاصة مع صعوبة الفصل بين النشاط الذي يتعلق بالاستخبارات، وجمع المعلومات، وحرب الفضاء الإلكتروني، أو التمييز بين الاستخدام السياسي والإجرامي، وتساهم البيئة المثالية تلك للفضاء الإلكتروني في عمل الجماعات المختلفة، ودعم القدرة على تشكيل شبكة عالمية، بدون سيطرة مباشرة، بالإضافة إلى "رخص التكلفة وسهولة الاتصال، وضعف الرقابة التقليدية عليه، ومثل

ذلك عنصر جذب لاستخدامها، وتوظيفها، لتحقيق أهداف سياسية وعسكرية. وساعدت البيئة المحلية والسياق الدولي للفضاء الإلكتروني على بروز الصراعات ذات البعد المحلي - الدولي من خلال توفير بيئة مناسبة لدمج الفئات والقوى المهمشة في السياسة الدولية وخلق شبكة تحالفات مؤيدة أو معارضة ذات نطاق دولي عريض: إما على أساس قيم حقوقية، أو انتماءات عرقية، أو دينية" (١٤).

وساهم الفضاء الإلكتروني في دعم الهيكل التنظيمي، والاتصالي، للحركات، والجماعات، والمنظمات المدنية؛ إلى جانب بروز ظاهرة الفاعلين من غير الدول في عمليات التجنيد، والحشد، والتعبئة، والتمويل.

وتتنقل الصراعات الممتدة عبر الفضاء الإلكتروني، وتتميز بحدوث حالات متكررة، للقرصنة المتبادلة، دون أن" تسفر عن حرب تقليدية بالضرورة؛ وخاصة مع صعود

دور "الفرد" في العلاقات الدولية، مثل حالة الصراع العربي الإسرائيلي، أو ما بين باكستان والهند، أو ما بين الصين والولايات المتحدة، أو ما بين الصين وتايوان، أو كوسوفا أو غيرها من مناطق الصراعات"(١٥).

ويمكن أن يستخدم الفضاء الإلكتروني "كوسيلة من وسائل الصراع داخل الدولة Inter State Conflict،بين مكوناتها على أساس طائفي، أو اقتصادي، أو ديني، وهو ما يساعد على كشف ديناميكيات التفاعل الداخلي إلى الخارج، بما يسهل من عملية الاختراق الخارجي، عبر شبكات الاتصال بدعم أحد أطراف الصراع بأدوات غير قتالية" (١٦)

وكان لتكنولوجيا الاتصال والمعلومات دور في وجود أهداف ووسائل جديدة، وأوجدت قابلية التعرض للهجوم، وهو ما أوجد نوعاً جديداً من الضرر دون الحاجة للدخول الطبيعي والمادي لإقليم الدولة، وذلك

لاعتماد الدول على الأنظمة الإلكترونية في كافة منشأتها الحيوية" بما يجعل من تلك الأنظمة هدفا للهجوم، وخاصة أن تلك الأنظمة تحمل طابعاً مدنياً وعسكرياً مزدوجاً ؛ وذلك بعد أن تمخض عن الثورة التكنولوجية ثورة أخرى هي الثورة في الشؤون العسكرية وتطور تقنيات الحرب" (١٧)

ومن هذا المنطلق نناقش في هذا الكتابالمحاور التالية:

- ماهية حروب الفضاء الإلكتروني من حيث المفهوم وأبرز الخصائص.

- أهم أدوات حروب الفضاء الإلكتروني المتمثلة بالقرصنة الإلكترونية.

- أثر حروب الفضاء الإلكتروني علي صراعات حروب الجيل الخامس.

- دور مواقع التواصل الاجتماعي في الحرب النفسية كأداة للتعبئة السياسية والتجنيد السياسي:

أولاً: ماهية حروب الفضاء الإلكتروني من حيث المفهوم وأبرز الخصائص.

إن الإنترنت هو نتيجة ثانوية للعلوم والتكنولوجيا في سباق الحرب الباردة، فبعد الحرب العالمية الثانية، تصاعد التوتر بسرعة بين الولايات المتحدة والاتحاد السوفياتي، وشكل إطلاق الاتحاد السوفييتي للقمر الصناعي سبوتنيك عام ١٩٥٧ إنذار خاصاً في الولايات المتحدة، حيث "غير هذا الإطلاق من تصور العالم من الولايات المتحدة كقوة تكنولوجية عظمى، وخلق شعور الضعف بين الشعب الأمريكي، ورفع المكانة الدولية للاتحاد السوفيتي" (١٨).

إن هذا الأمر، إضافة إلى تهديد الحرب النووية التي كانت تخيم على البلاد، قد دفع الحكومة الأمريكية إلى تغيير في الاستراتيجية التي أكدت "على التكنولوجيا والعلوم، من أجل تقليص الفجوة الملحوظة، حيث صُرفت الأموال في العلوم والهندسة والرياضيات

والتعليم والبحث على جميع المستويات .من بين المبادرات العديدة، أنشأت الولايات المتحدة ومولت وكالة مشاريع البحوث المتقدم (ARPA) Advanced Research Research Advanced Projects Agency التابعة لوزارة الدفاع بعد بضعة أشهر من إطلاق سبوتنيك، وكانت مهمتها المحافظة على التفوق التقني العسكري للولايات المتحدة ومنع "المفاجأة التكنولوجية"، ولقد أرادت إثبات قدرتها من خلال إنشاء شبكة الإنترنت"(١٩).

كان أبرز ما يقلق الجيش الأمريكي، هي القدرة النظرية لتوجيه ضربة نووية من قبل الاتحاد السوفيتي، لتعطيل أنظمة الاتصالات الأمريكية تماماً، لا سيما "أن هيكل القيادة والسيطرة في الحكومة الأمريكية والجيش، لا يمكن أن يصمد أمام مثل هذا الهجوم، وبالتالي، رأى محللون عسكريون ضرورة أنشاء شبكة اتصالات قوية من شأنها الصمود في أي مواجهة نووية، إذ

كان العنصر الحاسم، الذي يشكل مصدر البقاء، هو تقنية ما تسمى "الاتصالات الموزعة"، وهي موجودة تحت أنظمة الاتصالات التقليدية، مثل شبكات الهاتف، أي عملية تحويل البيانات من مدخلات الإنتاج" (٢٠).

ردا على هذا التهديد، الباحث في مركز أبحاث سلاح الجو، ومؤسسة راند، پول باران **Paul Baran**، تصور نظام توزيع يتكون من العقد ذات تبديل متعددة مع العديد من الروابط المرفقة. فبموجب نظام باران، إذا فشلت عقدة واحدة، فهذه المعلومات ليس لها سوى اتخاذ طريق بديل، هذا التكرار جعل قطع الخدمة للمستخدمين أكثر صعوبة، علاوة على ذلك، اقترح "باران" تحديد مكان وجود العقد بعيدة عن المراكز السكانية لجعل النظام أكثر أمناً. الأمر المهم في ذلك، وذات العلاقة بموضوعنا، هو خلق "باران" لتقنية التبديل بهدف نقل البيانات عبر الشبكة،" والذي شكل الأساس الذي تقوم عليه فكرة الإنترنت اليوم، الذي

يمثل مسرح الصراعات الحالية. لكن، مع الاندماج المتزايد بين أجهزة الكمبيوتر في حياة الأفراد جعل نقاط الضعف في الفضاء الإلكتروني واضحاً على نحو متزايد أيضاً، خصوصاً إذا ما علمنا، أن شبكة الإنترنت يتم تقاسمها بالكامل بين الاستخدامات المدنية والعسكرية في آن واحد، حيث تصاعد استغلال نقاط الضعف من خلال استخدام البرمجيات الخبيثة الارتكاب الجرائم الإلكترونية، الذي ترافق مع نمو الحوسبة الشخصية والإنترنت، مما أدى إلى ازدياد عدد وتأثير الجهات الفاعلة السيئة بشكل كبير" (٢١).

ومنذ عام ١٩٩١ أصبح الفضاء الإلكتروني يحمل معني أوسع وأشمل للتعبير من الانترنت، ليضم كل الاتصالات، والشبكات، وقواعد البيانات، ومصادر المعلومات، وأصبحت بنية النظام الالكتروني، تعني المكان الذي لا يعد جزءً من العالم المادي أو الطبيعي؛ حيث إنه ذات طبيعة افتراضية رقمية إلكترونية تتحرك

في بيئة إلكترونية حيوية، تعمل من خلال خطوط الهاتف، والكابلات الاتصالية، والألياف البصرية، والموجات الكهرومغناطيسية، ويمكن وصف العالم الالكتروني؛ بأنه "عبارة عن شبكات الكمبيوتر والاتصالات الالكترونية، وهو عبارة عن شبكة كمبيوتر خيالية، تحتوي علي كم هائل من المعلومات التي يمكن الحصول عليها، لتحقيق الثروة والسلطة؛ بحيث يصبح استخدامه محل نزاع بين الدول، ويعبر اختراقه تهديداً صريحاً لأمن ومصالح الدول أيضاً "(٢٢).

لذلك فقد تم إعادة التفكير دولياً في مفهوم الأمن، والذي امتد إلي حماية الدولة من التعرض للهجوم العسكري إلي حماية المنشآت الحيوية للبنية التحتية من التعرض لأعمال عدائية، من خلال استخدام تكنولوجيا الاتصال والمعلومات، وأصبحت قضية أمن الفضاء الالكتروني، تدخل في استراتيجيات الأمن القومي

للعديد من الدول المتقدمة للعمل علي الحيلولة دون تعرض بيئتها التحتية الحيوية للخطر (٢٣).

فقد أصبحت حرب الفضاء الالكتروني بديلاً عن الحرب المباشرة بين لدول، "وأصبحت القدرة علي القيام بهجمات الكترونية أداة سيطرة ونفوذ استراتيجية بالغة الأهمية، سواء في وقت السلم، أو في وقت الحرب، بسبب زيادة علاقة الفضاء الالكتروني، بعمل المنشآت الحيوية للدول - سواء المدنية، أو العسكرية، مما أدي إلي إمكانية تعرضها لهجمات الكترونية، تستهدف الشبكة، كوسيط، وحامل للخدمات، أو بشل أنظمتها المعلوماتية، مما يعرقل قدرتها علي القيام بوظائفها" (٢٤).

مما أدي إلي دخول المجتمع الدولي في مرحلة جديدة، تلعب فيها هجمات الفضاء الالكتروني دوراً أساسياً، سواء في تعظيم القوة، أو الاستحواذ علي عناصرها

الأساسية، "وأصبح التفوق في مجال الفضاء الالكتروني، عنصراً حيوياً في تنفيذ عمليات ذات فاعلية علي الأرض، وفي البحر، والجو، والفضاء من خلال نظم التحكم والسيطرة "(٢٥).

وقد زادت حالة الانكشاف الأمني للدول، نتيجة لاعتمادها المتزايد "علي الفضاء الالكتروني مختلف النشاطات، مثل برامج الحكومة الإلكترونية، والتي تصبح عرضة للاختراق، والهجوم بالفيروسات، وسرقة المعلومات وإتلافها"(٢٦).

وحالة الانكشاف الأمني هذه كانت بفعل ظهور الحواسيب، والشبكات، والذكاء الاصطناعي، وكلها مترابطة علي مستوي الكوكب كله، "فإن قيادة الحرب اليوم علي مجموعة اتصالية رقمية، لا مثيل لها تتكون من شبكات كثيفة، للرصد، والإعلام،

والاتصال، والتحديد الجغرافي، والتنصت الالكتروني، وفك الرموز، والتحليل، والمحاكاة "(٢٧).

بالنسبة لساحة حرب الفضاء الالكتروني، فنجد أن ساحة حرب الفضاء الالكتروني، هو جهاز الحاسوب المحمول، الذي يرتبط بكابل يربطه بأجهزة الخوادم، واليوم أصبح الفضاء الإلكتروني ساحة حرب تشهد كثيراً من المعارك الحاسمة في القرن الحادي والعشرين، وما يجعل من هذه الأماكن ساحة لقتال قوات حرب الفضاء الالكتروني، هو أن قوات حرب الفضاء الالكتروني، تستطيع أن تدخل في قلب هذه الشبكات، وتسيطر عليها، أو تدمرها، وإذا استولت علي شبكة ما، فإنه يمكنها أن تسرق كل معلوماتها، أو ترسل إليها تعليمات، بتحويل الأموال، أو تسريب لنفط وإطلاق الغاز، أو تفجير المولدات، أو إخراج القطارات عن قطبانها، أو صدم الطائرات، أو إرسال كتيبة، لتقع في كمين، أو تفجير في المكان الخطأ، أو "إخراج الأقمار

الصناعية عن مداراتها، ليذهب في غير هدي الفضاء السحيق، أو إيقاف رحلات الخطوط الجوية تماماً. وهذه الأمور ليست افتراضات فقد حدثت مثلها أحياناً علي سبيل التجريب، وأحياناً أخري علي سبيل التجريب، وأحياناً أخري علي سبيل حرب الفضاء الالكتروني. فالمعلومات التي تتعامل معها شبكات الحاسوب، والتي تدير المرافق، ووسائل المواصلات، والمصارف، يمكن استغلالها ومهاجمتها في ثوان، ولا تستطيع الجيوش، والأساطيل، الدفاع عنها، لأنها تقع في المجال الرقمي للفضاء الإلكتروني "(٢٨).

وإذا انتقلنا إلي تعريف حرب الفضاء الإلكتروني، فنجد أنه من الصعب تقديم تعريف محدد للفضاء الإلكتروني، فهناك العديد من الآراء المتفاوتة حول الطابع الذي يحدد الفضاء الإلكتروني، فهناك من يري بأنها:" حرب تخيليةٍ أو افتراضية virtual ٍReality ذات طبيعةٍ غير ملموسة، تحاكي الواقع بشكلٍ شبه

تام. وهي حرب بلا دماء، بحيث تتلخص أدوات الصراع فيها بالمواجهات الإلكترونية، والبرمجيات التّقنية، وجنود من برامج التخريب المحوسبة، وطلقات من لوحات المفاتيح ونقرات المبرمجين، في بيئةٍ اصطناعيةٍ تُحاول ما أمكن الوصول إلى صورة حقيقيةٍ لملامح الحياة المادية والملموسة "(٢٩).

ويعرف آخرون الحروب الإلكترونية بأنها:" المشهد الصراعي المستقبلي والقادم للبشرية، ولكن بصورة رقمية وتكنولوجية". وهي صراعات قديمة جديدة، بدأت منذ الوقت الذي ابتكر فيه الإنسان أدوات تواصله الأولى، كالأصوات، والتخابر، والتلغراف، والهواتف السلكية، وأنظمة البرق الصوتية، وأنظمة الترميز، وآلات الطباعة وغيرها، والتي تم استخدامها في الحربين العالميتين الأولى والثانية، وما سبقهما من حروب وثورات وقعت في عقدي الثورة الفكرية والصناعية (٣٠).

أكملت أدوات التواصل مسيرتها التطورية تبعاً للتقدم التكنولوجي الذي طرأ على المسيرة الإنسانية في عقودها اللاحقة، لتصل عقدنا الحالي، وتأخذ منحنى آخر، يرتكز في كونها أضحت "من أهم ما تتميز به البشرية في عصرها الحالي. بذلك، زادت هذه التطورات التّقنية والرقمية من رقعة الصراع الإلكتروني عبر الفضاء الرقمي، بوسائل أكثر فاعليةً وسرعةً وقوة" (٣١).

يزاوج البعض بين مفهوم الحروب الإلكترونية الدائرة في أنحاء الفضاء التكنولوجي، وما يعرف بالفيروسات البيولوجية Biological Viruses من ناحية آلية العمل، والتي تُصيب الإنسان بالأمراض. بحيث يتم تعريفها بأنها: " حرب الوحدات المركزية المتقنة العمل، "والتي تهدف إلى نشر الوباء الإلكتروني في جسم الضحية، عبر إرسال كميةً من المعلومات الرقمية الهادفة للتخريب، أو التنصت والتجسس ." وهي امتداد للأسلحة الجرثومية والبيولوجية التي شرع الإنسان

بابتكارها تزامناً مع انتشار الأسلحة النووية، ولكن بصورةٍ تّقنيةً والكترونيةً ومعلوماتية " (٣٢).

وهناك من يربط مفهوم الحرب الإلكترونية ببيئة الإنترنت فقط، كونها ساعدت على انتشار المعلومات في مختلف أرجاء المعمورة بشكل كثيف، وسهلت الوصول إليها بشكل سريع. بحيث يتم تعريف الحروب الإلكترونية بناء على ذلك بأنها :"الحرب التي تستهدف المعلومات،وهي تعبير عن الاعتداءات التي تطال مواقع البيانات الموجودة على الإنترنت، "وتحاول الاستيلاء على معطياتها، بين أطراف متناقضة الأهداف، ومتعارضة المصالح، ومختلفة المواقف" (٣٣).

يتفق المفهوم السابق الذكر مع الأبعاد السياسية والعسكرية التي" تتخذ من الفضاء الإلكتروني مسرحاً لتنفيذ أجندتها وأهدافها، بحيث تُستخدم تكنولوجيا المعلومات لإنجاز التفوق المعلوماتي، وحماية

الخطط الاستراتيجية، والبقاء بعيداً عن دائرة الإصابة الإلكترونية" (٣٤).

وفي نفس السياق العسكري، تُعتبر المجالات العسكرية من أكثر البيئات تجانساً والتصاقاً بالحروب الإلكترونية. تُعرف الحروب الإلكترونية تبعاً لهذا التناغم في المجالات بأنها " : الحروب التي تتم بالتعاون مع الحرب العسكرية، إذ أنها تصوب نيرانها "نحو الأهداف الإلكترونية والرقمية والمعلوماتية، كالتجسس على الإشارات الصادرة من الأجهزة الحاسوبية التابعة للفئات المستهدفة، وتتبع الموجات المنطلقة من الهواتف النقالة وغيرها ". وبالتالي، تستهدف هذه النيران الإلكترونية المصالح القومية والسياسية والعسكرية والأمنية للفئة المستهدفة، متخذةً لأجل ذلك شكل الهجمات الإلكترونية، أو الاختراقات الإلكترونية الهادفة لتعطيل البنية المعلوماتية لها" (٣٥).

يرى بعض القانونيين أن ديناميكيات عمل الحروب الإلكتروني ة تتقارب من ناحيةٍ قانونيةٍ مع إشاعة الرعب والإرهاب. لذلك، يمكن تعريف الحروب الإلكترونية استناداً لهذه النظرة القانونية بأنها : " نظام قائم على الرعب المنتشر في الشبكة العنكبوتية (الإنترنت)، "والتي تهدف إلى تنفيذ العديد من الأعمال لترويع أمن الأفراد والجماعات والمؤسسات والدول، وإرهاقهم اقتصادياً، وإدخالهم في أزماتٍ نفسيةٍ واجتماعية ناتجةٍ عما يعرف بالإرهاب الصامت" (٣٦).

ينطلق هذا المفهوم السالف الذكر من الو اقع الغربي، والذي له حيثياته ونظرته الخاصة في تفسير الإرهاب. ولكن، إذا رددنا هذا التعريف إلى محيطنا العربي؛ نُلاحظ أنه قد لا يتوافق ع العديد من التوجهات العربية، والتي تنظر إلى الفضاء الإلكتروني من عدة زوايا، "أهمها زاوية الحرية، والمتنفس التعبيري ضد ما يعانيه المواطن العربي في شتى الأقطار العربية من ظلمٍ

واستبداد. وزاوية المقاومة، والتي يحاول فيها الشباب العربي توظيف إمكانياتهم التّقنية في توجيه ضرباتٍ إلكترونيةٍ نحو إسرائيل، وهو أمر تعتبره الأخيرة ومن يواليها في العالم إرهاباً بحقها" (٣٧).

ينظر ذوي الاختصاص إلى الحرب الإلكترونية على أنها: "حرب العصر الحقيقية، مسارها الرئيس الشبكات الرقمية والإلكترونية، كذلك الوسائل التكنولوجية الأخرى، والأدوات الإعلامية، وكل ما يتعلق بعالم المعلوماتية والحداثة. الغاية الرئيسية لهذه الحرب هي الأضرار النفسية والمعنوية بالدرجة الأولى، ثُم تتبعها الأضرار المادية. وهي حرب ناعمةٌ، صامتةٌ، مظلمةٌ، بعيدةٌ عن الوسائل الحربية الخشنة، لكنها لا تُمانع في امتطاء الترسانات المسلحة والعسكرية الضخمة" (٣٨).

ويعتبر آخرون أن الحرب الإلكترونية هي امتداداً للحروب التقليدية والمادية، بحيث "يتألف جندها من المدنيين والعسكريين في آنٍ واحدٍ. كما أنها حرب أدمغةٍ بالدرجة الأولى، كونها تستهدف في المقام الأول تدمير البنية العلمية والمعلوماتية للهدف، وتأخذ أشكالاً عدة، كشكل الاتصالات بين الجيوش وقياداتها، وإضعاف شبكات النقل والإمدادات اللوجستية، وضرب المعلومات الاقتصادية، وإحراج الساسة، والعبث بالمحتوى التّقني والرقمي وغيرها" (٣٩).

يتضح مما تم عرضه من مفاهيم متعلقةٍ بالحرب الإلكترونية، بأن لها خمسة جوانب تحدد آلية عملها. أولها، أن هذه الحروب الرقمية تستهدف فئات معينة، قد تكون أفراداً، أو مؤسسات، أو منظمات، أو دول. وثانيها، أن بيئة المعلومات الرقمية هي المستهدفة في هذه الحرب. وثالثُها، أن "سلاح هذه الحرب هي النظم والوسائل الإلكترونية والاتصالية بشتى أنواعها.

ورابعها، أن لهذه الحرب تكاليف سياسية واقتصادية واجتماعية وأمنية باهظة الثمن. أما آخر هذه الجوا نب، فهو الجانب الأيديولوجي، والذي قد يعتلي ممارسات هذه الحرب في الفضاء الإلكتروني، ليلوح معرفاً عن هوية المهاجم، أو يفسر سلوك هذه الحرب بالإيجابي أو السلبي" (٤٠).

وثمة نقطة أخري جديرة بالإشارة نود أن نشير إليها، وهي أن بيئة عمل الحروب الإلكترونية على ما قامت به البشرية في عقدها المعاصر من تحولاتٍ نحو" تبني مفاهيم المجتمعات المعلوماتية المرتكزة على سلاسل ضخمةٍ من البيانات الرقمية والقومية الكُبرى، وشبكات الاتصال الحديثة، وانتشار الإنترنيت، وخدمات نقل المعلومات عبر البروتوكولات وقنوات التواصل، ومساعية في انتشار الأعمال التجارية الإلكترونية، والوثائق المحوسبة، وغيرها من الوسائل المعتمدة في عملها على البيئات الإلكترونية" (٤١).

ضمن هذا السياق المتنامي للثورة المعلوماتية؛ تشكلت بيئاتٍ تّقنية وإلكترونية ذات مدلولاتٍ توسعية وانتشاريةٍ رافضةٍ لعنصر التحكم والرقابة، ومنادية "بمزيد من الابتكارات الرقمية والمعلوماتية الاتصالية، والتي تصب في مفهوم الحداثة، وانصهار الحدود الجغرافية بين شعوب الأرض، مما ساعد وبشكلٍ كبير في تشكيل البيئات الرقمية الحاضنة للحروب الإلكترونية "(٤٢).

يدخل حصر أو تخصيص بيئة عمل الحرب الإلكترونية في العديد من الجدليات، شأنها في ذلك شأن الجدل الواقع على تفسير م فهوم الحروب الإلكترونية. فهناك من يرى أن اتساع رقعة الإنترنت، وانتشار استخدام تكنولوجيا المعلومات، قد "ساعد في انتشار الجرائم الإلكترونية Cybercrime، والتي لها أضرارها المالية والاجتماعية والنفسية والسلوكية والأخلاقية، إذ تُعرف هذه الجرائم بأنها : " اعتداءاتٌ حديثةٌ نسبياً، وذلك لارتباطها بعنصر التطور المعلوماتي

الحديث، وتمتاز بكونها متجددةً بصفةٍ دائمة، وذات أوجهٍ تكنولوجيةٍ متعددةٍ، وفائقة المرونة والتشغيل، وقد جلبت معها طائفةً جديدة مما يسمى بمجرمي المعلوماتية " (٤٣).

لا شك في أن للحداثة المعلوماتية والتكنولوجيا الاتصالية الحديثة تأثيراتها السلبية على المجتمعات الإنسانية.ولكن، يبقى عنصر توظيف المهارات التّقنية والاتصالية هو المحدد لوجهة عمل هذه التطورات في البيئات الرقمية. فمن غير الممكن المزاوجة بين من يستغل هذه التطورات في "إلحاق الأضرار بأفراد المجتمع، كسرقة الأموال، والعبث بأمن المعلومات القومية وغير القومية، لتحقيق أهدافه الشخصية، وبين من يوظف هذه الوسائل والتطورات كنوعٍ من المقاومة ضد الاحتلال، أو الدفاع عن وطنه من الغطرسة التكنولوجية التي تُمارسها كُبريات الدول في العالم "(٤٤).

تحتكم بيئات عمل الحروب الإلكترونية تبعاً لمدى توظيف الابتكارات التّقنية والرقمية في مثل هذه البيئات، مضافٌ إليها البعد الأخلاقي، والذي يكاد أن يكون شبه معدومٍ في البيئات الإلكترونية، حيث تُقسم بيئة الحروب الرقمية تبعاً لذلك إلى ثلاثة أقسامٍ وهي (٤٥) :

١ -بيئة حرب المعلومات الشخصية: والتي تكون ذات طابعٍ شخصي، هدفها التخريب والسرقة؛

٢ -بيئة حرب المعلومات بين الشركات: والتي تتخذ الطابع التنافسي بين الشركات؛

٣ -بيئة حرب المعلومات العالمية: تنشب بين دول العالم بعضها ببعض، أو بين عدة أطراف.

من الصعب وضع ملامح أو حدود لبيئة عمل الحروب الإلكترونية، نظراً للتطورات المتسارعة التي يشهدها قطاع تكنولوجيا المعلومات في عصرنا الحالي، علاوةً

على الإقبـال البشري الذي يشهده هذا القطاع، بين من هم مشيدون لهذا القطاع، أو من هم مشككون به. لذلك، "يختلف الباحثون في تحديد ملامح هذه البيئات إلى (مبالغين) بالمخاطر التي أوجدتها البيئـات الإلكترونية، مستندين على مؤشراتٍ حاسمةٍ خلفتها البيئات الرقمية، والتي ما زالت تُلقي بنتائجها على البشرية جمعاء. وبين من هم (مخفّفين أو ساخرين) بهذه البيئات، معولون على قدرة الإنسان بفرض رقاب ته وسيطرته عليها، ومنادون بأن هناك من يضخم سلبية هذه البيئات لتحقيق مآربه الشخصية" (٤٦).

يمكن القول هنًا، أن الفضاء الإلكتروني بشكلٍ عام، ومع ما يحتويه من بيئاتٍ رقميةٍ وتكنولوجيةٍ، تُشكل، بتداخلها معاً، ساحات الحروب المعلوماتية، وبيئات الصراعات الإلكترونية الناشئة عبر الفضاء الإلكتروني العالمي، والتي يتمثل أهمها بما يلي (٤٧):-

١ -الإنترنت: والذي يعد من أكثر البيئات الرقمية ملائمةً للحروب الإلكترونية؛

٢ -الترددات والموجات السلكية واللاسلكية : كتلك المنبعثة من وسائل الاتصالات المحمولة وغير المحمولة، والراديو، والموجهات الكهرومغناطيسية، ومحطات البث التلفزي، وغيرها

٣ -البنى المعلوماتية المحوسبة: لا سيما البنى التحتية المعلوماتية العسكرية والمصرفية والحكومية والاقتصادية والاجتماعية والسياسية، والمتبادلة رقمياً بوسائل الإنترنيت وأجهزة الاتصال الحديثة؛

٤ -الساحات الإعلامية، ووسائل الإعلان، وبيئات الإعلام الحديث؛

٥ -بيئة التكنولوجيات الحربية والعسكرية؛

٦ -الأقمار الصناعية ومراكز الاتصال والقيادة والسيطرة الرقمية، وغيرها الكثير من الوسائل.

وفيما يتعلق بعمل آلية تلك الحروب الإلكترونية، فنجد أنها تلوح في الأفق أفق عالمنا المعاصر، وتتجه العديد من حكومات دول عقدنا الحالي لانتهاج سياساتٍ تِّقنية ورقمية هادفةٍ لإنشاء إداراتٍ؛ خاصةٍ تُعنى بهذه الحرب العصرية، " كإنشاء مراكز متخصصة في إدارة شبكات الإنترنيت، وما يختلجها من قضايا تكنولوجيةٍ تستدعي الدول لأن تكون جاهزةً لتطبيق ما في جعبتها من خطط للحد من الهجمات الإلكترونية، أو الردع الإلكتروني، أو حتى محاولة السيطرة على منافذ توزيع الإنترنيت داخل حدودها القومية" (٤٨).

تقوم آلية عمل الحرب الإلكترونية بالدرجة الأولى على توفر عنصرين مهمين في أي صراعٍ إلكتروني قد ينشب في الفضاء الرقمي. أول هذه العناصر هي توفر المعلومات، والتي ترتكز عليها الحروب التكنولوجية بشكلٍ كبير." فتوفر عنصر المعلومات هو أول آليات عمل الحروب الإلكترونية. أما ثاني هذه العناصر، فهي

القُدرات العقلية والذهنية، والتي تكون مسؤولة عن تخطيط وتوجيه الضربات الإلكترونية، في عالمٍ رقمي شديد التعقيد، وزخم المعلومات"(٤٩).

قد يقول قائلاً، بأن توفر هذين العنصرين، هو مطلب أساسي لأي حربٍ في العالم، سواء كانت تقليدية أو ردعية أو إلكترونية. ولكن، نجاح عمل وسائل الاتصال الحديثة، وأدوات تكنولوجيا المعلومات المتطورة، والتي هي جنود الحروب الإلكترونية؛ "مرهون بتزويدها ببنية معلوماتية صحيحةٍ نابعة من عقلٍ بشري يعي أهدافه بشكلٍ سليم، لكي تتمكن من تصويب نيرانها الرقمية بشكلٍ دقيق، فبدون هذه التوأمة الثنائية، لن تستطيع أي حربٍ إلكترونيةٍ تحقيق أهدافها بصورةٍ رقميةٍ دقيقة، ولن تتمكن أدواتها من القيام بعملها بكفاءة وفاعلية شبه مطلقة" (٥٠).

يتبع توفر عنصري المعلوماتية والقُدرات العقلية البشرية، والتي تستند إليها آلية عمل الحروب الإلكترونية؛ الإجراءات الفنية والتّقنية، والقائمة على أساس تنفيذ خطوات وآليات الحرب الإلكترونية عبر الفضاء الرقمي، حيث تُقسم إلى ما يأتي (٥١) -:

١ -عمليات الهجوم الإلكتروني Electronic Operations Attack تنطلق هذه الهجمات من قاعدةٍ معلوماتيةٍ تقوم عليها معظم عمليات الحروب الإلكترونية في العالم، وهي العمليات المعلوماتية Information Operations تهدف هذه العمليات إلى السيطرة على معلومات الخصم، لمنعه من القيام بأي عمليات مسبقة، حيث يتم التركيز على ضرب معلوماته؛ أي الخصوم السياسية، والاقتصادية، والعسكرية، لإلحاق الأضرار المادية والمعنوية النفسية به؛

٢ -عمليات الدفاع الإلكتروني E-defense Operations، وتشمل الإجراءات والوسائل الوقائية، وذلك للحد من ردة فعل الخصم المهاجم. تتلخص هذه العمليات الدفاعية بالمنع والوقاية، والتي تهدف إلى حماية النظم المعلوماتية للطرف المهاجم، وتحذيره وتنبيهه، وكشف الاختراقات الرقمية في حال حدوثها، أو وضع الخطط الاستباقية الرامية لمنع وقع أي اختراقاتٍ معلوماتية.

ثانياً: أهم أدوات حروب الفضاء الإلكتروني المتمثلة بالقرصنة الإلكترونية.

لا شك في أن الأسلحة الإلكترونية أصبحت تستخدم بشكل متزايد ضد أهداف عسكرية ومدنية، ومن المهم معرفة أن الأسلحة الإلكترونية تأتي في الواقع في شكلين مختلفين: الأول هو طريقة التسليم الفعلي الأسلحة، وهو جهاز قياسي مستخدم فعلياً بمثابة البوابة الإلكترونية التي يتم من خلالها تنسيق الهجمات

الإلكترونية والأسلحة الإلكترونية التي تم تأسيسها. أما النوع الثاني من الأسلحة الإلكترونية هو عنصر الفضاء الإلكتروني. "هذه الأسلحة غير الملموسة يحتمل أن تكون مؤلفة من برامج الكمبيوتر، شبكة الفيروسات، وقيادة عمليات رقمية. على الرغم من التطور المستمر، فإن الأنواع الأكثر شيوعا من الأسلحة الإلكترونية، بما في ذلك وظائفها الأساسية، والقدرات، والاستخدامات، ترد في أدناه "(٥٢).

تبعاً لذلك، يمكن إجمال أهم أسلحة الحروب الإلكترونية وأساليب ها وأدواتها، والتي يتم استخدامها عبر الفضاء الإلكتروني كوسائل للحرب الإلكترونية أو غير الإلكترونية، إلى ما يلي:

١ -التجسس المعلومات **Spyware Information**

تُمثل وسائل التجسس التّقني والمعلوماتي أحد أشهر وأقدم أسلحة الحروب الإلكترونية، فقد تم استخدام

هذا السلاح منذ بداية الاستعمال الإنساني لوسائل الاتصال والتواصل. تتخذ وسائل التجسس المعلوماتي عدة أشكال، منها "ما يتم عبر التجسس والتنصت على المعلومات الصادرة من أجهزة الحواسيب، أو الصادرة عن المحطات الطرفية، أو اعتراض المراسلات الإلكترونية الصادرة عن الأقمار الصناعية، والهواتف المحمولة، وغيرها من وسائل التجسس المعلوماتي ذات الطابع القديم أو الحديث" (٥٣).

٢ -الحرمان من الخدمة: هجوم الحرمان من الخدمة DoS Denial of Serviceيعرف بأنه (اعتداء على الشبكة من خلال إغراقها بسيل من البيانات غير اللازمة أو طلبات إضافية ما يسبب بطء الخدمات أو توقفها تماما).عموما، "هجمات DOS تعمل من خلال شل موارد الموقع الإلكتروني على شبكة الأنترنت أو شبكة الكمبيوتر، وجعلها غير صالحة للاستعمال من قبل الأكثرية المستعملة لهذا المورد مع كمية هائلة

من طلبات الحصول على المعلومات، مما يؤدى إلى عدم القدرة على الاستجابة للمعلومات المشروعة وطلبات الحصول على البيانات" (٥٤).

إن نشر هجوم -الحرمان من الخدمة DOS يعمل على نحو مماثل لهجوم حجب الخدمة القياسية، ولكنه ينطوي على التنسيق واستخدام العديد من أجهزة الكمبيوتر المصابة قبل العمل في انسجام تام لتعطيل شبكة الكمبيوتر المستهدفة أو الخدمة على وجه التحديد، المعتدي " يستخدم الآلاف من أجهزة الكمبيوتر المصابة المعروفة باسم زومبي (zombies) لمهاجمة نظام واحد في وقت واحد. هجمات DDoS تبقى جذابة وسلاح فعال في الحرب الإلكترونية ألنها تزيد أضعافا مضاعفة عن قوة هجمات حجب الخدمة القياسية، وهي متوفرة بتكلفة منخفضة نسبياً " (٥٥).

بالإضافة الى ذلك، هناك هجوم حرمان دائم من الخدمة PDoS Permanent Denial of Service،هذا الهجوم يسبب أضرار جسيمة في النظام الأمر الذي" يتطلب استبدال أو إعادة تثبيت الأجهزة. خلافاً لهجوم دوس الذي يستخدم لتخريب خدمة أو موقع، أو كغطاء للتسليم البرامج الضارة، فإن هجوم PDoS يهدف بشكل محض الى تخريب الأجهزة" (٥٦).

٣ -البرامج الخبيثة، أو البرمجيات الخبيثة، تعمل عادة عن طريق (تعطيل وظائف الكمبيوتر العادية، أو عن طريق فتح باب خلفي لمهاجم بعيد من أجل السيطرة على جهاز الكمبيوتر) الفيروسات، هي الشكل الأكثر شيوعا من البرامج الخبيثة، قد تعمل لحذف ملفات معينة في الكمبيوتر أو جعل مثل هذه الملفات غير صالحة للاستعمال. على وجه التحديد، الفيروس يعلق نفسه على برنامج كمبيوتر أو ملف وينتشر من جهاز كمبيوتر إلى آخر، والانتقال عبر شبكات

الكمبيوتر عن طريق التكرار الذاتي. بالإضافة إلى ذلك، أن الفيروس عادة يحمل)حمولة) التي تمثل أحد الآثار الجانبية للفيروس، وعادة يعمل على إفساد أو تدمير بيانات الكمبيوتر على جهاز الكمبيوتر المصاب. الفيروسات عادة لديها القدرة على البقاء بسرية موجودة في جهاز الكمبيوتر المصاب، ليصبح مدمرا فقط عند تشغيل المستخدم أو يفتح البرنامج الذي قد تم إدراج البرنامج الخبيث فيه " النموذج المشترك الأخر من البرامج الخبيثة هي الدودة Computer worm، التي تؤدي وظائف مماثلة عن طريق الانتشار من كمبيوتر إلى آخر، وإصابة الفيروس في نهاية المطاف، شبكة الكمبيوتر بأكملها. مع ذلك، الدودة تختلف عن بكونها اسرع منها كما أنها قادرة على حد سواء في الانتقال عبر نظام الحاسوب دون مساعدة من مستخدمي الكمبيوتر وأنها قادرة على تكرار نفسها مباشرة

آلاف المرات داخل جهاز كمبيوتر واحد. الديدان تميل إلى أن تستهلك كميات هائلة من الذاكرة، ونتيجة لذلك، أجهزة الكمبيوتر المصابة، والشبكات، غالبا ما تصبح لا تستجيب. مع التطورات الأخيرة في مجال الأنترنت، الديدان قد تمنح الآن الأفراد نفق في أنظمة الحاسوب والسيطرة من بعيد على الكمبيوتر المصاب " (٥٧).

٤ -القنابل المنطقية، هي نوع أكثر تقدما من البرامج الخبيثة، وهي عبارة عن تعليمات برمجية ضارة مصممة بحيث تعمل عند حدوث أحداث معينة أو تحت ظروف معينة أو لدى تنفيذ أمر معين، وتؤدي إلى تخريب أو مسح بيانات أو تعطيل النظام ؛ " القنبلة المنطقية يمكن أن تبقى نائمة لفترات طويلة من الزمن لم تكن متصورة ومن ثم يتم تفعيلها، مما يجعل آثارها أكثر بكثير من أن تكون واسعة الانتشار. بمجرد تفعيلها، القنبلة المنطقية قد تسبب أضرارا

بالغة لجهاز الكمبيوتر المصاب، مما يجعله غير صالح للاستعمال تماما، وحذف بيانات محددة، أو حتى تعمل لتنشيط أكثر تعقيدا لهجوم DOS "(٥٨).

٥ -أحصنة طروادة، كما يوحي الاسم، تعمل كنوع من البرامج الضارة بناء على خداع أجهزة الكمبيوتر المستهدفة ودفعها إلى الاعتقاد أن برنامج خبيث سوف يؤدي، في الواقع، وظيفة مفيدة أو المطلوب منها. بدلا من ذلك، حصان طروادة يتمكن من الوصول الغير مصرح به إلى جهاز الكمبيوتر المصاب. في وقت لاحق، برامج حصان طروادة يسمح للمستخدم عن بعد الوصول إلى الكمبيوتر المصاب ويمكن أن "يسخر أيضاً جهاز الكمبيوتر المصاب ليكون بمثابة مورد في وقت الحق من هجمات DOS يمكن لأحصنة طروادة أن تسبب أضرارا خطيرة عن طريق حذف الملفات وتدمير المعلومات على النظام، كما يمكنها أيضا إنشاء باب خلفي على أجهزة الكمبيوتر التي تتيح

لمستخدمين البرنامج الخبيث الوصول إلى النظام، وربما السماح للتسوية المعلومات السرية أو الشخصية. على عكس الفيروسات والديدان، أحصنة طروادة ال تتكاثر عن طريق إصابة الملفات الأخرى كما أنها لا تكرر بالذات" (٥٩).

٦ -الاختراق الإلكتروني Penetration Mail وهي عبارة عن إنشاء نظامٍ أو برنـامجٍ إلكتروني يهدف إلى استغلال معلومات الخصم وتدميرها، إضافة إلى إفساد نظامه الحاسوبي والآلي، وذلك بهدف التقدم عليه أمنياً وعسكرياً واقتصادياً وسياسياً، "وقد تكون هذه المواجهة على المستوى الفردي، أو المؤسساتي، أو على مستوى الدول. للاختراق الإلكتروني أشكالاً عدة، لكن تتلخص جميعها بوظيفةٍ واحدة، وهي الدخول إلى قلب معلومات الخصم، والحصول عليها، مستخدمةً لأجل ذلك،

نظام محوسب يضرب البنية المعلوماتية للفئة المستهدفة" (٦٠).

٧ -زرع الفيروسات التّقنية في البيئات المعلوماتية : وهي عبارة عن برامج إلكترونية مدمرة، تعمل ضمن آلية معينة يحددها صانع هذه البرامج، ولها أشكال وأنواع متعددة. تهدف هذه الفيروسات الإلكترونية إلى إحداث فوضى في نظام تشغيل الضحية المنوي" ضربه إلكترونياً، وتلويث بيئته المعلوماتية، وذلك بغية تعطيل الوصول المعلوماتي للضحية، وفقدانه لغالبية مخزونه الرقمي، وربما ضرب الأجزاء المادية من أنظمة التشغيل الخاصة به" (٦١).

٨ -القرصنة الإلكترونية Electronic piracy تُعتبر القرصنة، من أضخم وأشمل الأسلحة الإلكترونية المستخدمة عبر الفضاء الرقمي. يشتمل هذا السلاح التّقني على غالبية وسائل الصراع الإلكتروني في

يومنا هذا، وذلك لشمولية مفهومه ومضمونه، حيث تقوم آلية عمله على تجنيد العديد من الأشخاص المؤهلين والقادرين على التعامل مع الحاسوب بخبرةٍ ودرايةٍ عاليةٍ جداً، تُمكنهم من اقتحام مختلف الوسائل الاتصالية، والنُظم التكنولوجية، من حواسيب، وهواتف، وموجات، وألياف ضوئية وغيرها. كما ويطلق على هؤلاء الأشخاص المؤهلين للعمل الحاسوبي والإلكتروني في عالم البرمجيات والإلكترونيات اسم الهاكرز Hackers؛

٩ -الرسائل الصامتة Messages silent عبارة عن برمجة تّقنية مخصصة للهواتف Generation Third وهي رسائل يتم برمجتها المحمولة الذكية من فئة الجيل الثالث بشكلٍ لا يشعر حامل الهاتف أو المحمول بوصولها، بحيث "تُساعد مرسلها على التحديد الدقيق لمكان تواجد الشخص، وذلك عبر استخدام معادلة تقوم باحتساب قوة إشارة الموجات

المنبعثة من الجهاز المحمول تبعاً لأقرب ثلاث مراكز مستقبلة لهذه الموجات ؛ أحدثت هذه التّقنية العديد من الأزمات في المجتمعات الغربية، كونها تحوي جانباً من التعدي على الخصوصية، وهو ما أثر على نسبة مبيعاتها في العالم، علماً أنها لاقت قبولاً ورواجاً من قبل رجال الأمن في بعض دول العالم" (٦٢).

١٠ -وسائل الإعلام: تلقى هذه الوسائل إقبالاً عالياً من قبل الجمهور المتلقي، نظراً لسرعة انتشارها، وكثرة متابعيها، وتأثيرها على النفس البشرية. دخلت هذه الوسائل عالم الحروب الإلكترونية عبر فضائيات التلفزة، ومحطات البث المحلي الملتقطة عبر الراديو، ومواقع الفيديو الاجتماعي كاليوتيوب YouTube،" والدوبلاج الكاريكاتيري Cartoon Dubbing،وغيرها من وسائل الإعلام الأخرى. تستخدم العديد من دول العالم هذه الوسائل بشكل كبير، خاصة في توجيه الخطابات

السياسية، وهي سلاح متعدد الأطراف، يتم توجيهه إلى دولة أو نظام أو مجموعةٍ بغية تهديدها أو تحذيرها أو التأثير عليها نفسياً ومعنوي" (٦٣).

١١ -شبكات التواصل الاجتماعي: وهي تركيباتٌ اجتماعيةٌ تّقنيةٌ ذات محتوى رقمي، تقوم بربط الحلقات الاجتماعية بعض ها ببعض، كالعمل والدين وغيرها، والتي تضم في طياتها مختلف الفئات العمرية، وجميع المستويات الاجتماعية والاقتصادية، وكافة الدرجات الثقافية والتعليمية (٦٤). وتضم شبكات التواصل الاجتماعي باقةً من المواقع ذات النفوذ القوي عبر العالم، من أشهرها: الفيس بوك، تويتر، اليوتيوب، البريد الإلكتروني، الماسنجر، غوغل بلس، المدونات الإلكترونية، وغيرها الكثير. تعد هذه المواقع من أكثر البيئات تناسباً وتناغماً مع الحروب الإلكترونية، وأكثرها اصطداماً وصراعاً، بل قد

تكون هذه الشبكات هي وجه الصراع الإلكتروني القائم الآن في عقدنا التّقني هذا، باعتبارها سهلة الوصول والاستخدام، وتفاعلية وشعبية بشكلٍ كبير، ومتطورة بوتيرةٍ مرتفعة. ومن المآخذ عليها أنها ذات طابع اصطيادي، أي يمكن من خلالها الإيقاع بالضحايا الإلكترونيين، إلا أنها وفي المقابل، منبراً حاشداً للتغيير السياسي "(٦٥).

١٢ -الأقمار الاصطناعية: Satellites وهي أسلحةٌ ذات دلالات استحواذيه، هدفها السيطرة على أكبر قدر ممكنٍ من المعلومات، وذلك عبر التقاط ملايين الصور للهدف، وإرسالها للقاعدة المعلوماتية الموجودة على الأرض. تعتبر الأقمار الاصطناعية من أكفئ الوسائل التّقنية، وأكثرها تعقيداً في حسم المعارك، فهي قادرةً على توجيه الصواريخ والقاذفات النارية صوب أهدافها على الأرض، وقد بلغت ذروة استخدامها إبان الحرب الباردة، والتي هددت العالم

باندلاع حرب كونية ثالثة. كما وتستخدم اليوم في التشويش على المحطات الفضائية، ومنعها من البث، وذلك بأجندة وأهدافٍ سياسية، في تعبير جديد عن الحرب الإلكترونية الدائرة في العالم الافتراضي، كالتشويش الذي تعرضت له بعض القنوات الفضائية العربية (العربية، الجزيرة) خلال الثورات العربية" (٦٦).

١٣ -الحقيبة الكهروستاتيكية Electrostatic bag : أحد أنوع التكنولوجيات العسكرية Military Technologies وهي عبارة عن أجهزة صناعية على شكل حقائب صغيرة، تقوم بتوليد نبضات كهرومغناطيسية Electromagnetic Pulses فائقة القُدرة، يمكن من خلالها تدمير الوحدات الالكترونية في أي ةِ إدارة أو محطة إرسال، مما يفقدها قُدرتها العملية والإنتاجية والتشغيلية. هناك أبحاثاً جاريةً عل ى هذه الحقيبة، وذلك "

بهدف تطوير نواتها الخاصة، والتي تُسمى الميكروبات Microbes إلكترونية، بحيث يتم تصويبها ضد التّقنيات السيليكونية Technology Silicon،بغية تدمر المعدات الالكترونية الخاصة بها"(٦٧).

١٤ -الخداع الإلكتروني E-Deception وهو من أهم وسائل تأمين الصراعات الإلكترونية، وبه تحقق المعارك الإلكترونية عنصر المفاجأة. يشتمل" هذا السلاح الرقمي على عدة وسائل، أهمها: التقليد الصوتي، التشويش الإلكتروني، التضليل المعلوماتي، الخداع ونشر الشائعات، انتحال الشخصيات افتراضياً، الابتزاز الإلكتروني، وغيرها من أساليب الخداع الرقمية" (٦٨).

١٥ -الغزو الفكري عبر الوسائط المفتوحة Open Mediaيقصد بالمصادر المفتوحة، تلك المصادر

المعلوماتية العامة والمتاحة للجميع، خاصةً المنتشرة على شبكة الإنترنت، كالمجلات، والنشرات، والتقارير، والكُتب الإلكترونية، والمدونات الرقمية، والألعاب الرقمية. يوظف القائمون على الحروب الإلكترونية هذه المصادر بطرقٍ متعددة، أشهرها ما يعرف بِ (استخبارات المصادر المفتوحة) Open Source Intelligence،والتي لا تتوقف عن جمع المعلومات، وتصنيفها، بل وإرسالها للمختبر المعلوماتي التحليلي، والذي يقوم بتوظيفها بشكلٍ فكري باتجاه الهدف المراد استخدام هذه الاستخبارات ضده. تُعتبر هذه المصادر من الأسلحة الإلكترونية مشرعنة الاستخدام، كونها متوفرة للجميع. ومع أنها تحوي جانباً بسيطاً من الاختراق الخُصوصي للإنسان؛ " إلا أن وزنها القانوني بسيط، كونها سهلة الوصول، ومتاحة للجميع. لذلك، كثيراً ما تُقدم عليها الجهات الأمنية والاستخباراتية

المختصة لسهولة الاصطياد المعلوماتي والأمني عبرها ، حيث تعج هذه الوسائط بالكثير من الأجندة المعلوماتية الرامية لزرع أوكار التجسس الإلكتروني، بعيداً عن دائرة التعقب القانوني والرقابي الهادف للإمساك بهذه الأوكار التجسسية الإلكترونية "(٦٩).

١٦ -الأسلحة النانو تكنولوجية-Nano Technology Weaponsيعد هذا المجال العلمي من أكثر المجالات إثارة، و أوعدها صعوداً، فهو يهتم بتصميم أجهزة تّقنية في غاية الدقة والصغر، وذلك من خلال رص الذرة بجوار الذرة للحصول على الشكل أو التكنولوجيا المطلوبة .تُسلط هذه التكنولوجيات العسكرية على الأجزاء المادية للأجهزة الحاسوبية والتّقنية Hardware ، بحيث تنتشر داخلها ، لتتسلل إلى أنظمة التشغيل، وتُفرغ ما بحوزتها من أنظمةٍ تدميريةٍ قادرةٍ على هدم البناء

المعلوماتي للنظام بسرعةٍ فائقة، في صورة تُشبه آلية عمل الفيروسات. لهذه الرقميات عدة أشكال، منها ما يعرف بالماكينات الدقيقة **Machinery Precision**،والتي تُخصص "لمهاجمة الأجزاء المادية للنظام المعلوماتي، ومنها ما يسمى بالميكروبات الرقمية **Microbes Digital**، والتي تُحدد لمهاجمة النظام التشغيلي لبيئة المعلومات المنوي استهدافها "(٧٠).

١٣ -الطائرات الإلكترونية (دون طيار): دخلت هذه الطائرات الحرب الإلكترونية، لتُشكل فوارق عديدةٍ في قُدرات الجيوش، ومدى امتلاكها للمنظومات المعلوماتية، والتي تؤهلها لتحقيق ما بحوزتها من أهدافٍ موضوعةٍ في بنكها المعلوماتي. تمتلك هذه الطائرات قُدرات عالية على التصوير والمراقبة، وحتى القصف بشتى أنواع القنابل. كما وتُشكل حلقات وصلٍ بين القاعدة المعلوماتية

الموجودة على الأرض، وساحة العمليات الحربية الكامنة في المجال الجوي والافتراضي، عبر مختبرٍ للتحليل المعلوماتي، والذي يمكنها من تحديد نيرانها بدقة. تُسمى هذه الطائرات عالمياً باسم (الطائرة دون طيار). أما فلسطينياً، فتُسمى بالطائرة الزنانة Drone Aircraft،حيث استخدمها الاحتلال الإسرائيلي ضد أهالي قطاع غزة، كما استخدمتها أمريكا في حربها على العراق وأفغانستان. يقول أحد الطيارين الأمريكيين عن هذه الطائرات الإلكترونية أثناء استخدامها في أفغانستان: "بإمكاننا مشاهدة العائلات حين ينهضون صباحا من نومهم وحين يذهبون لأعمالهم وحين يعودون لمنازلهم ويخلدون للنوم "(٧١).

١٤ -قنابل التعتيم الميكروويفية Blackout bom

يصوب هذا النوع من الأسلحة الإلكترونية نحو مولدات الطاقة، كالمزودات الكهربائية،

والـرادارات، ومحطـات التـزويـد بخدمات الإنترنيت، ومراكـز الاتصالات، والشبكات السلكية واللاسلكية، ومحطات البث الخليوي، وغيرها من وسائل تزويد الطاقة والمعلومات. يقوم مبدأ عمل هذه القنابل على إطلاق نبضاتٍ من الطاقة المغناطيسية قصيرة الموجة (الميكروويفية)، والتي تعمل على قطع كافة مصادر الطاقة والمعلومات في الكيان المستهدف، مما يؤدي إلى فصله عن العالم الخارجي، وبالتالي سهولة اقتحامه والسيطرة عليه بشكلٍ كامل. أحدثت مثل هـذه الأسلحة الجامعة بين مبادئ العمل الحربي والمعلوماتي صيحاتٍ إنسانيةٍ وحقوقيةٍ عديدةً في العالم، كونها تحوي العديد من التأثيرات السلبية على جسم الإنسان، ناتجةً عن الموجات التي تُ طلقها، والأصوات المزعجة الصادرة عنه" (٧٢).

١٥ -الأسلحة الروبوتية Robotic arms : جاءت التّقنية الحديثة بالكثيرِ من الطموح للإنسان، لتُقارب الفجوة بين الخيال والحقيقة، بل وتحول الخيال العلمي إلى حقيقةٍ واقعية قابلة للتطبيق والتنظيم والمحاكاة. تُعرف هذه الأسلحة الروبوتية بأنها : آلات يمكن التحكم بها عن بعد، "ويمكنها أن تتحرك بمفردها، بصورة تُحاكي الطبيعة الإنسانية. ازدادت هذه الوسائل تطوراً وتقدماً بفعل التقادم العلمي والتكنولوجي، لتدخل تدريجياً عالم الأعمال الحربية والمعلوماتية" (٧٣).

ويرى العديد من المراقبين أن هذه الآليات هي المشهد المستقبلي للحروب الإلكترونية والتقليدية والعسكرية على حدٍ سواء، حيث يعكف الخُبراء حالياً على وضع سيناريوهات لإسقاط آلاف من الأشكال الآلية في ساحات المعارك، كالرجال الآليين، والطائرات الآلية، والدمى الآلية، والمدرعات الإلكترونية وغيرها. جرت

التجربة على مثل هذه الروبوتات الآلية في أفغانستان من قبل القوات الأمريكية، حيث تم إطلاق الروبوت باكبوتسPackBots ، والذي يزن حوالي "٢٥ " كغم، ويدار عبر وسائل التحكم عن بعد، ومخصص لعلميات الاستطلاع ورصد السلاح الكيماوي، كما ويقوم بإطلاق الدخان كأحد وسائل التمويه. كما وجرت التجربة على روبوت آخر من قبل القوات الأمريكية في العراق، عرف باسم سترايكر StryKer، "ومزوداً بعجلاتٍ للدفع الثماني، ومخصص لعمليات نقل الجنود، لامتلاكه خاصية التحول إلى مدرعة متحركة على العجلات، والقيام بالعديد من الخدمات الميدانية الأخرى، والمتعددة المهام" (٧٤).

تتعدد وسائل وأنواع وألوان أسلحة الحروب الإلكترونية بمدى التقدم العلمي والتّقني الذي يواكبه الإنسان، فهو ينافس بني جنسه للحصول على أكبر قدر ممكن من هذه الأسلحة، وفي نفس الوقت، يصارع

الزمن من أجل وصوله إلى مرحلة استحواذ جميع ما تُنتجه البشرية "من هذه الوسائل المتقدمة. تجمع بعض الأسلحة الإلكترونية بين الطابع المعلوماتي والطابع الحربي العسكري، وبعضها الآخر، يقتصر عمله فقط عبر الشبكة العنكبوتية بكافة أشكالها وتخصصاتها" (٧٥).

ثالثاً: أثر حروب الفضاء الإلكتروني علي صراعات حروب الجيل الخامس.

يتحدث الكاتب الأمريكي "جون روب" في مؤلفه عن حرب الجيل الخامس بأن جنودها عبارة عن أفراد لا يرتدون الزي العسكري. وأنها حرب أفكار، وأنها تطلق دوامة من العنف، وتدار بأسلوب التدمير الفجائي لقوى الخصم معنوياً ونفسياً، بإطلاق عملية من شأنها إشاعة الإحباط لدى الخصم. وأن ميدانها هو الفضاء الالكتروني، وشبكات النت، لنشر مشاعر الخوف، وفقدان الثقة بالنفس لدى المجتمع، وأيضاً تجاه قادته

السياسيين؛ وتاريخياً نجد أن استونيا: خلال الحرب العالمية الثانية، وضع الاتحاد السوفيتي تمثال تذكاري من البرونز في عاصمة تالين لدولة إستونيا، وقد وجد الاستونيين أن عرض هذا التمثال يمثل رمزاً للاحتلال من قبل الاتحاد السوفيتي والقمع السياسي المرتكب في أعقاب الحرب العالمية الثانية، في حين أن روسيا تعتبر رؤية التمثال في إستونيا بمثابة تحية للجنود السوفييت الذين سقطوا في الحرب. في نيسان من عام ٢٠٠٧،قررت السلطات في استونيا إزالة هذا التمثال المثير للجدل، وقد كانت نتيجة هذا القرار ليلتين من الاحتجاجات وأعمال الشغب الجماهيري في إستونيا المعروفة باسم (ليلة البرونزي(في الأسابيع التي تلت ليلة البرونزي، شهدت البنية التحتية الرقمية في استونيا هجوم الكتروني واسع النطاق منشؤها في الغالب روسيا، علما أن إستونيا تعتبر واحدة من أكثر الدول التي تعتمد على الإنترنت في العالم،" ولقد استخدم "hacktivists" هجمات

DDoS ضخمة لاستهداف خوادم الويب في إستونيا وجعل حركة المرور في توقف تام، كما تضمنت الأهداف المحددة أيضاً الأخبار والمواقع الحكومية.

الهجوم ترك في نهاية المطاف الدولة في حالة من الفوضى، فبعد ساعات فقط من الهجوم، المواقع على شبكة الإنترنت من البنوك الرائدة في إستونيا، والصحف، والوكالات الحكومية الرئيسية تحطمت، مما دفع البلاد إلى العزلة في مجال الفضاء الإلكتروني. إستونيا تعتبر أول دولة تتعرض لهجوم منسق على نطاق واسع ضد أنظمة الكمبيوتر التي تديرها الدولة" (٧٦).

مما تجدر الإشارة اليه، أن هذه الهجمات قد نشأت من عدة دول أخرى، بهدف التمويه، الأمر الذي جعل تتبع المصدر النهائي مستحيلاً ؛ في نهاية المطاف، الهجوم على إستونيا أظهر عدة حقائق مثيرة للقلق، "لا سيما فيما يتعلق بمسألة الإسناد في الهجمات الإلكترونية، وسهولة

الهجمات الإلكترونية وتدمير العالم الحقيقي سببها هجمات نفذت فقط في مجال الفضاء الإلكتروني" (٧٧).

أما في جورجيا؛ فقد بدأت الحرب الروسية الجورجية في ليلة ٢ آب ٢٠٠٨، بعد أشهر من التوتر المتصاعد، ولقد تميزت بداية الأعمال العدائية المفتوحة بأجراء قصف على بلدة أوسيتيا الجنوبية تسخينفالي من قبل الجيش الجورجي ردا على الإجراءات الانفصالية، حيث شنت هجمات جوية وبرية مفاجئة ضد القوات الثورية التي تقع في محافظات أوسيتيا الجنوبية وأبخازيا، ولقد ردت روسيا بسرعة على حملة القصف بهجمة مرتدة ضخمة. خلال هذه الحرب القصيرة، تم استخدام الهجمات الكترونية إلى جانب الثالوث الحركي الذي تضمن هجمات جوية، أرضية وبحرية، الهدف الرئيسي من الحملة الإلكترونية كان لدعم الغزو الروسي لجورجيا من خلال استهداف البنية التحتية الحيوية. لقد كان حجم الهجمات الكترونية على مستوى عال من الأهمية،

حيث تم مهاجمة ما يقارب أربعة وخمسين من المواقع الجورجية بصورة اجمالية، ولقد كانت جميعها تقريبا من شأنها أن تنتج فوائد للجيش الروسي. أن الهجمات الإلكترونية استهدفت مباشرة العناصر الإعلامية والاقتصادية للسلطة الوطنية، المواقع الحكومية، المؤسسات المالية الجورجية، جمعيات رجال الأعمال، بالإضافة إلى موقع وزارة الخارجية الجورجية وغيرها من المواقع الحكومية الرئيسية بما في ذلك الرئاسة والوزارات والمحاكم والبرلمان، وقد شملت ايضا استهداف وسائل الإعلام ومرافق الاتصالات، والتي عادة ما قد تعرضت للهجوم من قبل صواريخ أو قنابل خلال المرحلة الأولى من الغزو،" بهدف منع الوصول إلى الأخبار والمواقع الحكومية، بالإضافة إلى جعل الأمر أكثر صعوبة لإجراء تقييم الأضرار في ساحة المعركة وتنسيق الاستجابات الفعالة. بالإضافة إلى ذلك، كان للهجمات الكترونية آثار نفسية هامة من خلال خلق حالة من

الذعر والارتباك في السكان المحليين. لقد كانت شدة الهجمات الإلكترونية كافية لتدفع الحكومة الجورجية الى نقل خوادم لمواقع الحكومة على الأنترنت الى كل من أستونيا والولايات المتحدة في محاولة لإحباط استمرار هجمات DDoS " (٧٨).

في الحقيقة ان القدرة على تحقيق التزامن بين كل من الهجمات الإلكترونية والهجمات العسكرية التقليدية يجعل من فعالية التدمير مزدوجة.

٣ -إيران: ستكسنت Stuxnet من البرامج الخبيثة التي تم استخدمها لمهاجمة منشأة لتخصيب اليورانيوم الإيراني في ناتانز، لقد تم الكشف عنه لأول مرة في حزيران ٢٠٠٩ من قبل الباحثين في أمن الحاسوب،" وقد اكتشف العديد من إصدارات حتى منتصف عام ٢٠١٠.على الرغم من أن تعريف الأسلحة الإلكترونية أمر دقيق، فان الخبراء في مجال الأمن الإلكتروني

نظروا في هجوم ستكسنت باعتباره أول برهان ملموس على قدرة الأسلحة الإلكترونية" (٧٩).

إن أجهزة الطرد المركزي المستخدمة في محطة ناتانز لتخصيب اليورانيوم كانت المستهدف الحقيقي من قبل ستكسنت، ومن أجل الوصول إلى هذه الأجهزة كان على ستكسنت أن يصيب أجهزة الكمبيوتر ذات العلاقة بالتحكم الصناعي المستخدمة في برمجة وسيطرة البرامج الآلية التي تسيطر على محولات تردد أجهزة الطرد المركزي. "لقد قام ستكسنت باستغالل نقاط الضعف في نظام التشغيل مايكروسوفت ويندوز قبل إصابة الجهاز بأكمله، من خلال استغلال الثغرات في تطبيق البرمجيات المتعلقة بوحدات البرمجة الآلية، لكي تأمر محولات التردد بالإضرار بأجهزة الطرد المركزي" (٨٠).

مما تجدر الإشارة اليه، أن أجهزة كمبيوتر التحكم الصناعي التي كان يجب على ستكسنت إصابتها لم تكن متصلا مباشرة إلى شبكة الإنترنت، حيث أن بروتوكولها الأمني يسمح فقط باستخدام الوسائل المادية والكهربائية أو الكهرومغناطيسية لعزل الأنظمة الأخرى، ولا سيما الإنترنت، ولقد كان من الضروري، مع ذلك، السماح للمشغلين أو الشركات بتحديث البرمجيات لارسال أو استرداد البيانات أجهزة الكمبيوتر، وللقيام بذلك، كانوا يستخدمون، "كما هو الحال في كثير من الأحيان، مفاتيح USB لذلك، قد تم تصميم ستكسنت للاستفادة من هذه العادة، حيث أنه أصاب مفاتيحUSB ،مما أدى إلى انتشار دودة بين أجهزة الكمبيوتر على الشبكة المحلية. ستكسنت تم بثه من ثلاث موجات من الهجمات ضد خمس منظمات موجودة في إيران، ثم انتشر إلى العديد من الشبكات

حتى وصل إلى أجهزة الكمبيوتر التحكم الصناعي المسئولة عن التنفيذ"(٨١).

مطوري ستكسنت اتخذوا العديد من التدابير للحد من انتشاره، فعلى عكس غيره من البرامج الضارة، ستكسنت لم يكن دودة، "فهو لم يكن مصمم للانتشار في أسرع وقت ممكن في الإنترنت، بل كان أنتشاره من خلال مفاتيح USB وضمن شبكة محلية وكل العنصر المصاب لا يمكن أن يصيب سوى ثالثة أخرى من العناصر. ستكسنت كان يحتوي على التعليمات البرمجية التي تشير إلى أن (تدميره) يكون في ٢٤ يونيو ٢٠١٢ " (٨٢).

في الحقيقة، أن العوامل التي تفسر انتشار ستكسنت تكمن في نقطتين أساسيتين :"الأولى، غياب تصحيح أو معالجة نقاط الضعف في ويندوز والأخرى تتعلق بطريقة

استخدام مفتاح USB التي كانت غير آمنة وعلى نطاق واسع"(٨٣).

توخيا للدقة، إن كان ستكسنت أصاب جميع هذه الأنظمة، ليس هناك دليل على أنه أتلف أنظمة في أماكن أخرى غير إيران. أن تحليلات التعليمات البرمجية لستكسنت "من قبل مجتمع أمن المعلومات خلصت إلى أن ستكسنت كان مبرمجا فقط للتشغيل ضد أجهزة الكمبيوتر التحكم الصناعية المستخدمة في أجهزة الطرد المركزي الإيراني في ناتانز" (٨٤).

إذا وكما رأينا، أن هذه الهجمات المتعلقة بالفضاء الإلكتروني لها عواقب هائلة على الدول المستهدفة، الأمر الذي" يثير العديد من التساؤلات حول حق الدول المتضررة في استخدام القوة العسكرية؟ كذلك، القانون الواجب التطبيق في هذه النزاعات الحديثة؟ لا سيما أنه

لحد الآن لا يوجد نص محدد للتعامل مع هذه الأسلحة الجديدةط (٨٥).

رابعاً: دور مواقع التواصل الاجتماعي في الحرب النفسية كأداة للتعبئة السياسية والتجنيد السياسي:

تتأثر أفعال وتحركات المكونات السياسية في نشاطاتها المتعددة بالعديد من المتغيرات الكونية والتكنولوجية المتطورة التي تتفاعل سلباً أو إيجاباً في حركتها الصراعية في المجتمع الدولي،" وهذا ما يبرر الجانب التقني والمعلوماتي كفاعل مهم في تغيير استراتيجيات العمل السياسي بشقيه العنيف والناعم، فضلاً عن أن الفضاء الإلكتروني المفتوح ساحة جديدة للأداء السيسي المرتبط بالهدف الاستراتيجي للدولة، وبما يعبر عن قدرتها وإجراءاتها المؤثرة علي الخصم" (٨٦).

فقد كانت الحرب بمفهومها العسكري إحدي أهم الوسائل المتاحة لفض الصراعات القائمة وفرض الإرادات، وحتي وقت قريب تدخلت فيه بعض المتغيرات

التي أثرت علي اتجاهات السياسة في الاعتماد المطلق علي الحرب المباشرة، أو الصدام المسلح كعامل فاعل لتأمين غاياتها، ومن بين تلك المتغيرات، التطور الكبير الذي" طرأ علي وسائل الاتصال ونقل المعلومات، جعل عالم اليوم صغيرا للحد الذي يستطيع فيه المرء أن يري أحداثاً تقع في مختلف أنحائه لحظة وقوعها وهو جالس في بيته، مما جعل هذه الوسائل ذات تأثير كبير علي تشكيل الآراء والتوجهات والقناعات ويمكن استثماره وبأقل ما يمكن من الخسائر" (٨٧).

إن هذا التطور الكبير في وسائل الاتصال أثر بشكل ملحوظ علي رؤية العديد من دول العالم، ودفعتها إلي التفكير بوسائل جديدة قادرة علي إحداث فعل التأثير علي تشكيل الآراء والقناعات المناسبة، وتكوين الاستجابات المطلوبة،" التي تتوافق في واقع الحال ومساعيها الحثيثة لتسيير مصالحها الاستراتيجية بطرق مقبولة لا تثير احتمالات المقاومة كما يحدث عادة في

التعامل مع الأساليب القديمة المتمثلة بالحرب التقليدية وبكلفة أقل بالمقارنة مع الكلف الباهظة للحروب التقليدية، وسعة تدمير أقل بالمقارنة مع تلك الحروب" (٨٨).

ولذا فقد بات التعامل علي المستوي النفسي يحتل الحيز الأكبر بين الأسلحة المستخدمة حاليا في النظام الدولي الذي ظهر فيه فاعلين دون مستوي الدولة، وذلك للتأثير علي وعي المستهدفين،" أخذت فيه الحرب النفسية إطاراً أكثر شمولية، وأبحت فيها الفضاء الإلكتروني أحد أدواتها المعروفة والأكثر استخداما، وبات استخدام المعطيات الإلكتروني النفسية السرية والعلنية الوسيلة الأكثر فاعلية لإيجاد القناعات والآراء والاتجاهات التي تسهل تأمين المصالح وتعين علي إدارة وتحليل القناعات والآراء والاتجاهات التي تسهل تأمين المصالح وتعين علي إدارة وتحليل الصراع" (٩٨).

وقد أصبحت النصوص الإلكترونية والوسائط الإعلامية المختلفة هي "المجال الأوسع تطبيقاً في حروب الجيل الخامس، وأصبحت السيطرة علي الساحات الافتراضية وخطوط الشبكة العنكبوتية والتحكم فيها، الوسيلة الأكثر فاعلية لتحقيق الأهداف المرجوة، الأمر الذي أدي تعدد أشكال ووسائل حرب الفضاء الإلكتروني" (٩٠).

لقد ظهرت ضرورة الاهتمام بأمن الفضاء الإلكتروني بسبب الاستخدام الكبير لتكنولوجيا المعلومات في عمل العديد من المرافق الحيوية، "مما يعرضها لخطر الهجمات الإلكترونية، كما شاع استخدام الفاعلين من غير الدول للفضاء الإلكتروني الذي يتعدي كل الحدود لتحقيق أهدافهم، مما كان له أثر سلبي في سيادة الدولة، ثم برزت إشكاليات تعامل الدول مع الشركات التكنولوجية متعددة الجنسيات، مثل مواقع الشبكات

الاجتماعية، كالفيس بوك، والتويتر، واليوتيوب، التي أصبحت فاعلين دوليين" (٩١).

ويمكن النظر للتغيير السياسي والاجتماعي برؤية(حتمية) التحول في ثلاثة مسارات : أولهما : ما يعرف (بالحتمية التقنية) **Technological Determinism**، وثانيهما : ما يعرف (بالحتمية الاجتماعية **Social Determinism**،" وإن لكلا المسارين وجهات النظر تدعم تفسيره، إلا أن التفسير الذي قدمه بعض المفكرين في اختلاف معدل التغير في كل من الثقافة المادية واللامادية نتيجة الـاثير التقني في المجتمعات يعد الأساس في التحليل الاجتماعي لتقنية الاتصال، مع احتمال حدوث تصادم بين التغيير التقني والتغير الثقافي، ويترتب عليه خلل وظيفي مما يؤثر في تفكير أفراد المجتمع، وتتوتر القيم والايديولوجيات السائدة" (٩٢).

فأمام عجز الأحزاب السياسية وجمعيات المجتمع المدني عن أداء أدوارها المتمثلة بالتعبئة بسبب الأنظمة الحاكمة من جهة، وغياب الديمقراطية الداخلية من في معظمها من جهة أخري، وتحولها إلي كائنات ذات أهداف آنية من جهة ثالثة، عم نفور المواطنين منها، لذلك فإن الوسائط الحديثة المتمثلة في الفضاء الرقمي استطاعت أن تحل محلها،" إذ لعبت دورا أساسيا في الحراك السياسي والاجتماعي الذي شهدته المنطقة العربية مع الانتفاضات الشعبية، وأسهمت بشكل كبير في نقل الوقائع الميدانية بشكل مباشر. وكذلك في تعبئة المحتجين وتنظيمهم عن طريق تسهيل التواصل فيما بينهم، ولن الشباب هم الكتلة السكانية الكبر في المجتمعات العربية، والأكثر شعوراً بالحرمان النسبي، والأكثر قدرة علي التواصل والحركة، فلم يكن مستغربا أن يكونوا في طليعة المحتجين" (٩٣).

بالإضافة إلي تسخير الجماعات الإرهابية الشبكة الرقمية والفضائيات لأغراضها الدعائية، منذ شرع تنظيم القاعدة قبل نحو عقد من الزمن في بث بياناته عبر الانترنت وبعض القنوات التلفزيونية العربية والعالمية، وحتي برز في السنوات الخمس الأخيرة، نشاط "رقمي " فعال للجماعات المتطرفة، لتسويق بياناتها وصور فعالياتها عبر مواقع التواصل الاجتماعي، " لا سيما " فيسبوك"، وتويتر"، في سعيها لتعزيز استراتيجية لا تهدف إلي نشر ثقافتها المتطرفة والتكفيرية فحسب، بل إلي شن حرب نفسية للتأثير في الخصوم، والسعي إلي استقطاب الشباب، للتطوع في صفوفها والقتال في البلدان التي تحارب فيها مثل أفغانستان، والعراق، وسوريا، واليمن، ودول أخري" (٩٤).

فقد أدي الانتشار الهائل في استخدام مواقع التواصل الاجتماعي إلي إحداث " ثورة كبري" تترك تأثيراتها علي كافة جوانب الحياة، ومن بينها الأمن الوطني للدول

الذي أصبح يواجه تحديات وتهديدات جديدة، بحيث توسع مفهوم الأمن الوطني ذاته ليتجاوز نطاق مواجهة التهديدات العسكرية وضمان حماية الوطن ووحدته وسلامة أراضيه وسيادته، إلي مجالات أخري تشمل الاستقرار السياسي والاقتصادي والانسجام الاجتماعي وسلامة البيئة، "ففي عام ٢٠١١، أعلنت وكالة مشروعات البحوث الدفاعية المتطورة DARPA عن برنامج لاستخدام مواقع التواصل الاجتماعي في تحقيق التواصل الاستراتيجي من خلال تحسين فهم وزارة الدفاع لما يجري علي مواقع التواصل الاجتماعي في الوقت الحقيقي له، خاصة في المناطق التي تنتشر فيها قوات أمريكية، فضلاً عن قيام وزارة الدفاع الأمريكية باستخدام مواقع التواصل الاجتماعي في بث رسائل إعلامية تخدم مصالحها الاستراتيجية" (٩٥).

أما فيما يخص دور مواقع التواصل الاجتماعي في أيدي التنظيمات الإرهابية، فلا شك في أن ظاهرة الإرهاب

تحظي باهتمام الشعوب والحكومات في شتي أنحاء العالم لما لها من آثار خطيرة علي أمن الدول واستقرارها، بعد أن اتضح أننا أمام ظاهرة إجرامية منظمة تهدف إلي خلق جو عام من الخوف والرعب والتهديد باستخدام العنف ضد الأفراد والممتلكات، مما يعني أن هذه الظاهرة الخطيرة تهدف إلي زعزعة استقرار المجتمعات والتأثير في أوضاعها السياسية وضرب اقتصاداتها الوطنية عن طريق قتل الأبرياء وخلق حالة من الفوضي العامة،" بهدف تضخيم الأعمال الإرهابية وآثارها التدميرية في المجتمع، بما يتناسب مع القاسم المشترك الذي أمكن التوافق عليه بين تعريفات الإرهاب، والذي يري في الإرهاب استخدام غير مشروع للعنف يهدف إلي الترويع العام وتحقيق أهداف سياسية، ما جعل البعض ينظر إلي الإرهاب باعتباره عنف منظم نحو مجتمع ما، أو حتي التهديد بهذا العنف، سواء أكان هذا المجتمع دولة أو مجموعة من الدول أو جماعة سياسية أو عقائدية علي

يد جماعات لها طابع تنظيمي تهدف إلي إحداث حالة من الفوضى وتهديد استقرار المجتمع من أجل السيطرة عليه، أو تقويض سيطرة أخري مهيمنة عليه لصالح القائم بعمل العنف في إشارة إلي اعتماد الإرهاب المفرط علي العنف المتعمد وعدم التمييز بين المدنيين وغير المدنيين كأهداف شرعية من أجل تحقيق أغراض سياسة" (٩٦).

وتعد ممارسة القوة عبر الانترنت إرهاباً إذا صاحبتها دوافع سياسية، مثل التأثير في القرارات الحكومية أو الرأي العام، ويتم ذلك من خلال ثلاثة أبعاد مهمة، يتمثل أولهما في توفير المعلومات عن الأهداف المنشودة لتنفيذ عمليات إرهابية تقليدية، فهو مساعد للإرهاب التقليدي، أو كوسيط في عمليات التنفيذ، أما البعد الثاني فيستخدم فيه الفضاء الإلكتروني للتأثير في المعتقدات، مثل التحريض علي بث الكراهية الدينية، وحرب الأفكار، في حين يتم البعد الثالث في صورة رقمية، حيث تقوم الجماعات المتطرفة علي اختلاف أشكالها

باستغلال مزايا الفضاء الإلكتروني كعنصر حيوي لدعم وتحقيق أهدافها، ومنفذ لوجستي داعم وحاضن لنشاطها الإعلامي في مناطق مختلفة من العالم(٩٧).

وفي هذا الصدد يمكن القول إن الجيل الحالي من مقاتلي التنظيمات الإرهابية، مثل تنظيم القاعدة وداعش، جيل مختلف عن الجيل الأول من المقاتلين، الذي كان يرتكز في عمليات التجنيد علي العلاقات الشخصية والتفاعل وجها لوجه بين أشخاص ينشرون خطاباً محرضاً علي العنف، ويستخدمون الأفكار والمبادئ الدينية والقناعات الفكرية لتجنيد الأعضاء، أما الجيل الحالي فهو نتاج ثقافة الإنترنت، "فمن خلال تويتر علي سبيل المثال يقوم شباب التنظيم بتداول الخبار أو المقاطع المصورة التي تحث علي نصرة الدين والجهاد علي مواقعهم، وجعلها متاحة لأكبر عدد من المتابعين الذين يقومون بدورهم بإعادة التغريد، ومن ثم تصل إلي آلاف المتلقين، ليس فقط في العالم العربي، بل في العالم

أجمع، وهو ما يفسر تمكن القاعدة وداعش من تجنيد شباب من المسلمين الذين يعيشون في الغرب" (٩٨).

وإمعانا في خلق أجواء الفوضي والترويع، وإتاحة المجال أمام انتشار الشائعات المغرضة، التي تثير خوف الرأي العام وتوليه ضد السلطات المحلية بحجة عجزها عن حماية آمنها، يعمد الإرهابيون إلي التسلح بوسائل الإعلام المختلفة لتسويق أغراصهم وغاياتهم وتوظيفها في تضليل الأجهزة الأمنية واكتساب السيطرة علي الرأي العام عن طريق نشر أخبار العمليات الإرهابية التي يقومون بتنفيذها، علي اعتبار أن الحملات الإعلامية التي تغطي هذه العمليات تساعد عي تحقيق استكمال وأهداف الإرهابيين، "الذين يرون في التغطية الإعلامية لجرائمهم معياراً هاماً لقياس مدي نجاح فعلهم الإرهابي، لدرجة أن البعض اعتبر العمل الإرهابي الذي لا ترافقه تغطية إعلامية عملاً فاشلاً، من هنا يأتي استغلا الإرهاب للإعلام لترويج فكرة الإرهابي ودعمه من خلال

محاولاته المستمرة في البحث عن الدعاية الإعلامية لتسليط الضوء علي وجوده وأغراضه " (٩٩).

ويستخدم الإرهابيون مواقع التواصل الاجتماعي نظراً لما تتيحه لهم من قدرة علي التواصل مع الآخرين؛ وبخاصة من فئة الشباب عبر العالم لبث أفكارهم بطرق مدروسة بشكل دقيق لإقناع هؤلاء الشباب بذلك الفكر المتطرف سواء من خلال الدين أو المبادئ التي يروجون لها أو الأفكار المتطرفة التي تتسم بالعنف في منهجها، "وتستغل اندفاع وطاقات الشباب ورغبتهم في الوصول للأفضل، وعدم إلمامهم بتلك الأفكار ومعرفتهم لهويتها في تضليلهم واجتذابهم للإيمان بها، ومن ثم جعلهم عناصر فاعلة في تنفيذ عملياتهم الإرهابية كل في وطنه وهو ما يتيح لهم انتشارا واسع النطاق في كل العالم بالإضافة لعدم قدرة الأجهزة الأمنية علي رصد نلك العناصر التي يتم تجنيدها عبر الإنترنت، حيث لا يتم

التعرف عليها، إلا عندما يقومون بارتكاب عملياتهم الإجرامية" (١٠٠).

فتعمد التنظيمات الإرهابية في استهدافها الشخصيات العامة والمسئولين الحكوميين علي نوعية المعلومات المنشورة علي شبكات التواصل الاجتماعي والتي تقترب إلي حد كبير من نشر تفاصيل عن مجريات الحياة اليومية لمستخدمي هذه الشبكات، قد أسهم في إمكانية استخدام هذه المعلومات لأغراض إرهابية، "من خلال استهداف الشخصيات العامة والمسئولين من جهات سيادية، من خلال رصد تحركاتهم، ومتابعة ذويهم وعائلاتهم، وهو ما يُعرض المسئول ومن حوله لخطر الاستهداف، ودون مبالغة الأمن القومي للبلاد"(١٠١).

وعلي الرغم من عدم الإعلان حتي الآن عن ثبوت استهداف إحدى المنشآت المدنية أو العسكرية من خلال متابعة شبكات التواصل الإجتماعى وصفحاتها الخاصة

من قبل الإرهابيين، فإن ثمة سوابق دولية في هذا الإطار ؛ فهجمات مومباي عام ٢٠٠٨ أعلن أنها قد تمت من خلال المتابعة والاعتماد علي معلومات كانت تنشرها نائب مساعد وزير شئون الدبلوماسية عن أماكن تواجدها علي صفحتها الخاصة علي " فيس بوك"، وقد استفاد منها الإرهابيون في القيام بعملياتهم. "وهو أمر يدعو إلي توخي الحذر من قبل العاملين في الجهات الحيوية في الدولة، ويستوجب الحرص في نشر الصور والإعلان عن أماكن التحرك والتواجد بشكل يسهل من مهمة الإرهابيين الذين اعتمدوا خلال الفترة الأخيرة علي عمليات استهداف الشخصيات العامة، والإعلان عن قائمة اغتيالات تضم مسئولين وشخصيات عامة" (١٠٢).

وهذا المحتوي الإلكتروني الذي يتم بثه من خلال تلك المواقع يمكن أن يشكل تهديد لأمن الدول والأشخاص وبخاصة الدردشة الإلكترونية والتي يمكن من خلالها أن يتم تبادل المعلومات الماسة بالأمن القومي وتجنيد

الشباب للعمل ضمن الخلايا الإرهابية والتنظيمات المتطرفة التي تعمل لحساب قوي معادية تستهدف أمن الوطن واستقراره، ويتم تجنيد الشباب واغواؤهم عن طريق المنتديات وصفحات التواصل عبر الفيس بول وتويتر وهو ما يشكل تهديدا كبيرا خاصة بالنسبة للعاملين في الهيئات الحيوية للدولة لمحاولة استدراجهم أو تجنيدهم سواء بالفكر المتطرف والدخول إليهم عن طريق الدين والجهاد في سبيل والهادة والجنة، أو استدراج الأفراد لنشر معلومات خاصة بهم ووظائفهم من خلال الفيس بوك أو تويتر، ثم دراسة جوانب شخصياتهم من خلال ما يقومون بنشره علي صفحاتهم الشخصية لتحديدهم وسيلة للوقوع في براثن الإرهابيين واقناعهم بالقيام بأعمال إرهابية تضر المجتمع والدولة، ومن أسباب جاذبية مواقع التواصل الاجتماعي للتنظيمات الإرهابية (١٠٣):

١ -قدرتها علي تحقيق التواصل الاجتماعي مع الاخرين بكل اللغات والثقافات لمختلف شعوب العالم.

٢ -عدم وجود رقابة علي التواصل بين أطراف الاتصال.

٣ -تتميز الاتصالات بالخصوصية.

٤ -إقبال الشباب علي هذه الوسيلة بشكل كبير.

٥ -انتشار المواقع الفكرية لرموز الفكر التكفيري وتواصلها بخطاب تحريضي جذاب مع زوارها ومعتنقي هذه الأفكار.

٦ -يعلم المتطرفون الجدد أن رموز الفكر التكفيري لم يعرفوا بشكل جماهيري إلا عن طريق المواقع الإلكترونية التي روجت لأفكارهم واستقطبت الاتباع.

٧ -تشكل المنتديات الحوارية المتطرفة وقود الصراع الفكري للفكر المتطرف مع خصومه بل إن بعض هذه المواقع يكاد يتجاوز عدد زواره ربع مليون زائر في إجازات نهاية الأسبوع.

٨ -تشكل القوائم البريدية التي يشرف عليها مديرو المواقع الإلكترونية حلقة الوصل بين أقطاب الأفكار المضللة والأتباع الذين بنشرون هذا الفكر في دوائرهم الخاصة وهو ما يعزز من تأثيرها.

يلاحظ أن الجماعات الإرهابية خلال الفترة الأخيرة بدأت في الاستفادة بشكل كبير من قدرة وسائل التواصل الاجتماعي علي نشر محتويات مخطط الحرب ضد أجهزة الدولة، وليس أدل علي ذلك من الذي نشره تنظيم "أنصار بيت المقدس" الإرهابي لمجزرة كرم القواديس بسيناء في أكتوبر ٢٠١٤، والذي استشهد علي إثرها ٣١ من جنود القوات المسلحة المصرية، من خلال تفجير الكمين بواسطة سيارة ملغومة، ثم قيام مسلحين بمهاجمة الجنود الذين نجوا من التفجير، وقتلهم، والاستيلاء علي كمية كبيرة من الأسلحة والذخائر النوعية التي كانت موجودة في الموقع، "والحقيقة أنه لا يمكن النظر لقيام التنظيم بتصوير تلك العملية وغيرها،

وبثها علي المواقع والصفحات الخاصة به، علي أنه تصوير لمجرد توثيق للحظة، والتأكيد علي أنه من قام بها، ولكن هدف التنظيم من خلال إقدامه علي هذه الخطوة إثارة الذعر والخوف، خاصة أن هذا التنظيم أعلن مبايعة لتنظيم الدولة الإسلامية " داعش" الذي يستخدم نفس الأسلوب" (١٠٤).

ويعد "تويتر" أحد أهم وسائل التواصل الاجتماعي التي تستخدم للتفاعل والتنسيق أثناء العمليات الإرهابية، وتكمن الميزة الأساسية في " تويتر" في أنه يوفر مجتمعات افتراضية متغيرة، تتكون بصورة تلقائية خلال الأحداث الكبري، وهو ما تستفيد منه تلك اجلماعات من خلال متابعة أحداث المعلومات عن أي قضية تظهر في المجال العام. ولعل المثل البارز علي ذلك هو الهجوم الإرهابي في مومباي في ٢٦ نوفمبر ٢٠٠٨، "والذي راح ضحيته نحو ١٦٤ شخصا، وجرح أكثر من ٣٠٠ شخص، وقد كشفت التحقيقات أن جماعة " عسكر طيبة"

الباكستانية كانت تقوم بالتنسيق مع منفذي الهجوم من باكستان، وإبلاغهم بالتطورات التي تحدث كافة من خلال الاعتماد علي أحدث الأخبار المنشورة علي تويتر، مثل تحركات وتمركز وحدات مكافحة الإرهاب الهندية "(١٠٥).

المنظمات الإرهابية تستخدم مواقع التواصل الاجتماعي كأداة لتحديد أهدافها والتعرف عليها ومراقبة تحركاتها، خاصة في إطار عمليات الاغتيالات في الدول المستهدفة، وذلك إما بمراقبة من يمتلك حسابات علي تلك المواقع، أو مراقية دائرة أصدقائهم ومعارفهم للوصول إليهم، وجمع البيانات اللازمة عن تحركاتهم، وتوفير الوقت والجهد اللازمين للقيام بذلك علي أرض الواقع، وأيضاً لضمان سرية المراقبة، ومن ثم، تعد وسائل التواصل الاجتماعي مهمة" لتلك الجماعات في إطار ما أسماه البعض " شبكات الكوادر" والتي تعمل علي التواصل بين كوادر التنظيم المسلح كأداة عابرة

لقيود المكان، وذلك من أجل مهام منها التدريب علي تكوين خلايا تنظيمية، واستقطاب مزيد من الكوادر وتدريبهم علي استخدام الأسلحة، والتنسيق للعمليات المسلحة وتوقيتها، والتدريب علي صنع القنابل البدائية وغيرها " (١٠٦).

وعلي صعيد آخر فإن مؤسسات الدراسات والأبحاث الدولية تستخدم مواقع التواصل الاجتماعي في جمع المعلومات والتحليل للمنظمات الإرهابية ومناصريها، من خلال استعمال برامج متخصصة في هذا المجال.

فمن خلال مواقع التواصل الاجتماعي (تويتر)، تمكن معهد أبحاث Rand للأمن القومي، من استحداث قاعدة بيانات كبيرة تميز بين مناصري الدولة الإسلامية في العراق والشام، فبالرغم من أن الدولة الإسلامية في العراق وسوريا ISISطلبت من أتباعها أن يشيروا إليها باستخدام تسمية" الدولة الإسلامية"، إلا أن من يذمونها

يستخدمون التسمية المختصرة " داعش"، وباستخدام عينة من بيانات تويتر تغطي فترة عشرة أشهر، "استخدمت المؤسسة التحليل اللغوي في سبيل دراسة المحتوي والمواضيع الرئيسية لدي المستخدمين الذين يستعملون عبارة "داعش" بمقابل أولئك الذين يستعملون عبارة " الدولة الإسلامية" في تغريداتهم، فتم الوصول إلي نتيجة أن المحتوي لدي مستخدمي عبارة " داعش" بكثرة شديد الانتقاد للدولة الإسلامية في العراق وسوريا، فالمستخدمون استعملوا مصطلحات مثل، داش الإرهابية، والخوارج، ومقاتلوا داعش، وكلاب النار، وكلاب البغدادي، لكن مستخدمي عبارة" الدولة الإسلامية" استعملوا مصطلحات متوهجة مثل، مجاهدي التوحيد، وجنود الخلافة، واسود الدولة الإسلامية"(١٠٧).

هوامش الكتاب

() عباس بدران: الحروب الالكترونية الاشتباك في عالم المعلومات، مركز دراسات الحكومة الالكترونية، بيروت، لبنان، ٢٠١٠، ص ٤.

(٢) وليد غسان سعيد جعلود : دور الحروب الالكترونية في الصراع العربي الإسرائيلي، رسالة ماجستير غير منشورة في التخطيط والتنمية السياسية بكلية الدراسات العليا في جامعة النجاح الوطنية نابلس، فلسطين، ٢٠١٣، ص ١ -٢.

(٣) شموئيل إيفن وآخرون: حرب في الفضاء الالكتروني: اتجاهات وتأثيرات على إسرائيل، تقديم وترجمة، محمود محارب، تل أبيب : معهد دراسات الأمن القومي، على: المركز العربي للأبحاث ودراسة السياسات (معهد الدوحة) ٢٠١١.

(٤) د.نـورة شـلوش: القرصـنة الالـكترونيـة في الفضـاء السيبراني التهديد المتصاعد لأمن الدول، مجلة مركز بابـــل للدراســـات الانســـانية، ٢٠١٨، المجلـــد: ٨، العدد:٢.، ص ١٩٣.

(٥) نفس المرجع، ص ١٩٣.

(٦) نفس المرجع، ص ١٩٣.

(٧) نفس المرجع، ص ١٩٤.

(٨) عادل عبد الصـادق: أسـلحة الفضـاء الإلكترونـي في ضـوء القـانون الـدولي الإنسـاني، أوراق، العـدد ٢٣، سلسلة تصدر عن وحدة الدراسات المستقبلية بمكتبـة الاسـكندرية، الاسـكندرية، ٢٠١٦، ص٩.

(٩) نفس المرجع، ص٩.

(١٠) د.نورة شلوش: نفس المرجع، ص ١٩٥.

(١١) نفس المرجع، ص ١٩٥.

(١٢) نفس المرجع، ص ١٩٥.

(١٣) نفس المرجع، ص ١٩٦.

(١٤) نفس المرجع، ص ١٩٦.

(١٥) نفس المرجع، ص ١٩٦.

(١٦) نفس المرجع، ص ١٩٦.

(١٧) نفس المرجع، ص ١٩٧.

(18) Michael Gervais, Cyber Attacks and the Laws of War, berkeley journal of international law, Vol. 30:2, 2012، p.527.

(1٩) ibid, Vol. 30:2, 2012، p.527.

(٢٠) ibid, Vol. 30:2, 2012، p.527.

(٢١) ibid, Vol. 30:2, 2012، p.527.

(٢٢) ماجد محمد الحنيطي : الحرب الإلكترونية وأثرها علي الصراعات الدولية المعاصرة، رسالة دكتوراه غير منشورة بكلية عمادة الدراسات العليا ، جامعة مؤتة، الأردن، ٢٠١٦ ،ص ٥٨.

(٢٣) ibid ص ٥٨.

(٢٤) نفس المرجع، ص ٥٩.

(٢٥) نفس المرجع، ص ٥٩.

(٢٦) نفس المرجع، ص ٥٩.

(٢٧) نفس المرجع، ص ٥٩.

(٢٨) نفس المرجع، ص ٦٠.

(٢٩) وليد غسان سعيد جعلود : نفس المرجع، ص ٨١.

(٣٠) نفس المرجع، ص ٨٢.

(٣١) نفس المرجع، ص ٨٢.

(٣٢) نفس المرجع، ص ٨٢.

(٣٣) نفس المرجع، ص ٨٢.

(٣٤) نفس المرجع، ص ٨٣.

(٣٥) نفس المرجع، ص ٨٣.

(٣٦) نفس المرجع، ص ٨٣.

(٣٧) نفس المرجع، ص ٨٤.

(٣٨) نفس المرجع، ص ٨٤.

(٣٩) نفس المرجع، ص ٨٤.

(٤٠) نفس المرجع، ص ٨٥.

(٤١) نفس المرجع، ص ٨٥.

(٤٢) نفس المرجع، ص ٨٦.

(٤٣) نفس المرجع، ص ٨٦.

(٤٤) نفس المرجع، ص ٨٦.

(٤٥) نفس المرجع، ص ٨٧.

(٤٦) نفس المرجع، ص ٨٧.

(٤٧) نفس المرجع، ص ٨٨.

(٤٨) نفس المرجع، ص ٨٨.

(٤٩) نفس المرجع، ص ٨٨.

(٥٠) نفس المرجع، ص ٨٩.

(٥١) نفس المرجع، ص ٨٩.

(٥٢) Bradley Raboin, Corresponding Evolution: International Law and the Emergence of Cyber Warfare, Journal of the National Association of Administrative Law Judiciary -31-2,Fall 2011,p. 610-611.

(٥٣) وليد غسان سعيد جعلود : نفس المرجع، ص ٩٨.

(٥٤) د. حسام عبد الأمير خلف: البعد الجديد ـ الخامس ـ في النزاعات المسلحة ـ الفضاء الالكتروني، ٢٠١٦، ص ١٢١.

(٥٥) نفس المرجع، ص ١٢١.

(٥٦) نفس المرجع، ص ١٢١.

(٥٧) نفس المرجع، ص ١٢٢.

(٥٨) نفس المرجع، ص ١٢٢.

(٥٩) نفس المرجع، ، ص ١٢٢.

(٦٠) وليد غسان سعيد جعلود : نفس المرجع، ص ٩٩.

(٦١) نفس المرجع، ص ٩٩.

(٦٢) نفس المرجع، ص ٩٩.

(٦٣) نفس المرجع، ص ١٠٠.

(٦٤) نفس المرجع، ص ١٠١.

(٦٥) نفس المرجع، ص ١٠٢.

(٦٦) نفس المرجع، ص ١٠٣.

(٦٧) نفس المرجع، ص ١٠٣.

(٦٨) نفس المرجع، ص ١٠٣.

(٦٩) نفس المرجع، ص ١٠٤.

(٧٠) نفس المرجع، ص ١٠٤.

(٧١) نفس المرجع، ص ١٠٥.

(٧٢) نفس المرجع، ص ١٠٥.

(٧٣) نفس المرجع، ص ١٠٦.

(٧٤) نفس المرجع، ص ١٠٧.

(٧٥) نفس المرجع، ص ١٠٧.

(٧٦) د. حسام عبد الأمير خلف: البعد الجديد ـ الخامس ـ في النزاعات المسلحة ـ الفضاء الالكتروني، ٢٠١٦، ص ١٢٥.

(٧٧) نفس المرجع، ص ١٢٦.

(٧٨) نفس المرجع، ص ١٢٧.

(٧٩) نفس المرجع، ص ١٢٧.

(٨٠) نفس المرجع، ص ١٢٧.

(٨١) نفس المرجع، ص ١٢٨.

(٨٢) نفس المرجع، ص ١٢٨.

(٨٣) نفس المرجع، ص ١٢٨.

(٨٤) نفس المرجع، ص ١٢٨.

(٨٥) نفس المرجع، ص ١٢٨.

(٨٦) ماجد محمد الحنيطي : نفس المرجع، ص ١٠٧.

(٨٧) نفس المرجع، ص ١٠٧.

(٨٨) نفس المرجع، ص ١٠٧.

(٨٩) نفس المرجع، ص ١٠٨

(٩٠) نفس المرجع، ص ١٠٨

(٩١) نفس المرجع، ص ١١٧.

(٩٢) نفس المرجع، ص ١١٧.

(٩٣) نفس المرجع، ص ١١٨.

(٩٤) نفس المرجع، ص ١١٨.

(٩٥) نفس المرجع، ص ١١٨.

(٩٦) نفس المرجع، ص ١١٨.

(٩٧) نفس المرجع، ص ١٢٣.

(٩٨) نفس المرجع، ص ١٢٤.

(٩٩) نفس المرجع، ص ١٢٤.

(١٠٠) نفس المرجع، ص ١٢٤.

(١٠١) نفس المرجع، ص ١٢٥.

(١٠٢) نفس المرجع، ص ١٢٥.

(١٠٣) نفس المرجع، ص ١٢٦.

(١٠٤) نفس المرجع، ص ١٢٦ - ١٢٧.

(١٠٥) نفس المرجع، ص ١٢٧.

(١٠٦) نفس المرجع، ص ١٢٧.

(١٠٧) نفس المرجع، ص ١٢٨.